



Всемирная паутина российского и китайского контроля за информацией

Валентин Вебер

Research Affiliate, Centre for Technology and Global Affairs, University of Oxford

Information Controls Fellow, Open Technology Fund

ориг. название: The Worldwide Web of Chinese and Russian Information Controls

автор: Valentin Weber

АННОТАЦИЯ

Повсеместное распространение китайских и российских методов и технологий контроля за информацией неоднократно становилось темой для первых полосы крупнейших газет мира.¹ Однако в этих публикациях не был представлен систематический анализ как движущих сил, так и последствий подобного распространения. В процессе подготовки настоящего доклада такой анализ был проведен, и одним из его выводов стало понимание, что контроль за информацией более эффективно распространяется в странах с гибридными и авторитарными режимами, особенно имеющими связи с Китаем или Россией. Китайская модель контроля за информацией легче распространяется среди стран инициативы «Один пояс — один путь»; российскую модель перенимают страны Содружества Независимых Государств. В начале доклада описаны российская и китайская модели контроля за информацией. Затем отслеживается их распространение в 110 странах, входящих в китайскую или российскую сферы влияния, где внедряются российские или китайские технологии контроля за информацией, методы управления информацией и соответствующие законы.

ВВЕДЕНИЕ

Технологии и методы, используемые Пекином и Москвой для контроля за информацией, вышли на глобальный уровень. В качестве примера экспортируемых технологий можно привести оборудования для цензуры или для строительства «умного города»; один из методов — рецепция китайского или российского права в данной области. Влияние технологий и методов заметно как в малых островных государствах с населением в 80-100 тысяч человек, вроде Антигуа и Барбуды, так в Индии с населением более миллиарда.² Пока журналисты с Багам, из Лесото и Перу проходят пропагандистские тренинги в Пекине, китайские механизмы наблюдения разворачиваются военным командованием на востоке Бразилии и в парламенте Иордании.³ Российское оборудование для слежки, в свою очередь, разворачивается как в пограничных


странах - Беларуси, Казахстане и Украине, так и в далеких от России, например, в Алжире, на Кубе, в Мексике и Палестине.⁴

Исследуя столь широкое распространение методов контроля за информацией, важно понять, почему российские, а не китайские технологии и методы применяются в одних странах, но не попали в другие? Что именно в том или ином подходе к контролю повышает вероятность его распространения в отдельных регионах? Есть ли разница в восприятии странами конкретного метода контроля? Какую выгоду получают Пекин и Москва от повсеместного распространения своих технологий?



Карта 1: Распространение российских и китайских средств контроля

Чтобы ответить на эти вопросы, в начале данного доклада вводится типология контроля за информацией. Во второй главе описывается типология российского и китайского подходов к контролю за информацией. В третьей главе мы раскрываем, как происходит измерение распространения. Четвертая глава иллюстрирует факторы распространения. В пятой главе отслеживается и анализируется распространение китайских и российских технологий, в том числе




имитация методов, законов, а также образовательные программы. В шестой главе описаны политические, экономические и интеллектуальные преимущества, которые получают Китай и Россия от экспорта технологий информационного контроля, а также воздействие на страны-импортеры. В заключении представлены рекомендации, как демократии могут смягчать последствия возможного злоупотребления контролем за информацией в будущем.

1. ТИПОЛОГИЯ КОНТРОЛЯ ЗА ИНФОРМАЦИЕЙ

Определения контроля за информацией предлагали многие исследователи. Одни концептуализировали контроль за информацией как «действия в киберпространстве или через него, направленные на прекращение, противодействие, манипуляцию информационным взаимодействием и коммуникации в стратегических и политических целях».⁵ Другие категоризировали контроль за информацией на страх (т.е. самоцензуру), препятствия (похоже на цензуру), и переизбыток (аналогично стратегическому распространению информации).⁶ В отличие от этих исследований, в данном докладе в центре концепта контроля за информацией находится слежка; исследуется, как слежка воздействует на другие формы управления информацией. Контроль за информацией может принимать разные формы, в их числе слежка, цензура, самоцензура и стратегическое распространение информации. Если изучить то, в какой степени та или иная страна *использует* различные формы контроля за информацией и какими *возможностями* (инструментами) контроля владеет, можно сформулировать несколько моделей контроля за информацией.

Слежка

Слежка является ключевой в единой концепции контроля за информацией. Благодаря ей работают цензура, самоцензура и стратегическое распространение



информации. Без слежки нет устрашения. Без нее, власти не знают, какой вебсайт следует блокировать и какие онлайн-дискуссии требуют «политического управления».

Слежка бывает открытой и скрытой. Когда население понимает, что за ним следят, может заработать самоцензура. Стоит отметить, что видимые проявления слежки не всегда требуют, чтобы она была эффективной. Власти могут устанавливать муляжи камер, чтобы пугать граждан. Но и слежка, незаметная для граждан, может давать результат. Незаметная слежка используется для блокировки специфического контента (цензура) или прямого стратегического распространения информации среди конкретных получателей.

Теории, рассматривающие контроль за информацией, но опускающие вопросы слежки, являются неполными. Излишний фокус на контенте и происходящем онлайн (например, фильтрация по ключевым словам) мешает оценить существенное влияние технологий на мир оффлайн (например, физический контроль через камеры наблюдения). В последние годы киберпространство (онлайн) слилось с физическим миром (оффлайном). Биты и байты, единицы и нули определяют свойства привычных предметов. Контроль за информацией превращается в физический контроль из-за повсеместного присутствия камер видеонаблюдения, систем умного города и других кибер-физических систем. Эксперт по кибербезопасности Брюс Шнайер (Bruce Schneier) максимально сжато описал эту ситуацию: «Интернет — это уже не сеть, к которой мы подключаемся. Мы живем в нем, это компьютеризированный, сетевой, взаимоподключенный мир. Это будущее, которое мы называем Интернетом вещей».⁷ Автомобиль теперь является конгломератом компьютера с прикрепленными к нему стальными деталями и колесами; и этот повседневный предмет добавлен в инструментарий слежки. К примеру, китайские автопроизводители передают властям информацию о местоположении и другие данные об электромобилях в режиме реального времени.⁸ Сегодня в Китае электромобили стали инструментом слежки, но их превращение в инструмент физического контроля

является, по всей видимости, лишь вопросом времени. Поскольку онлайн и оффлайн миры так тесно связаны, все действия человека онлайн — то, что он говорит, пишет и слушает — тесно переплетены с тем, что он делает в повседневной жизни (то есть, там, что мы ранее определили бы как оффлайн мир).

Самоцензура

Самоцензура возникает из правовых и неправовых (устрашение) наказаний, а также из страха, что слежка будет использоваться против отдельных людей или организаций (например, с помощью маркировки их властями как диссидентских).⁹ Хотя страх безусловно является ключевым фактором, запускающим самоцензуру, он не всегда сопровождает каждый факт самоцензуры. «Человек может воздерживаться от высказывания своего мнения в потенциально враждебной среде по разным причинам: это может быть попытка избежать спора, озабоченность чьими-то чувствами или риск обидеть человека, опасения относительно возможной потери работы или физической атаки в будущем, нежелание выглядеть человеком с особенным поведением».¹⁰ В рамках этого доклада, самоцензура определена как «отказ от высказывания собственного мнения в окружении, воспринимаемом как несогласное с этим мнением».¹¹ Чем больше инструментов для слежки находится в распоряжении государства, тем больше у него возможностей подтолкнуть население к самоограничениям.

Цензура

Цензура, то есть «подавление *другими* [выделено в оригинале] передачи точек зрения, воспринимаемых этими иными как враждебные или оскорбительные», может принимать разные формы.¹² Она может происходить на более тонком уровне, например, доступ к информации может быть усложнен снижением скорости отдельных онлайн-сервисов (например, Тор) или снижением места в выдаче поисковыми машинами нежелательного политического контента.¹³

Цензура может быть более широкой и менее разборчивой, если речь идет об отключении социальных медиа, служб сотовой связи или доступа в интернет.¹⁴

Цензура меняется с изменением возможностей слежки. Большая мощность инструментов наблюдения дает больше возможностей для цензуры.


Правительства с меньшими возможностями могут прибегать к отключению сетей для ограничения информации, правительства с большими возможностями предпочтут сделать информацию менее доступной, убирая её ниже в поисковой выдаче.

Стратегическое распространение информации

Стратегическое распространение информации включает в себя использование государствами пропаганды и дезинформации для управления общественным мнением на стратегическом уровне. Под пропагандой мы имеем в виду «публично распространяемую информацию, служащую для влияния на чужие убеждения и/или действия», в то время как дезинформация понимается как «недостоверная информация, распространяемая осознанно и злонамеренно».¹⁵ В контексте данного исследования примером дезинформации является создание и распространение «новостей», что СПИД был результатом экспериментов правительства США.¹⁶ Пример пропаганды от китайского правительства — влияние на микроблоги,¹⁷ обычно используемые для обмена изображением, видео и текстом. Популярная платформа для микроблогинга - Sina Weibo.¹⁸ Как и с цензурой, стратегическое распространение информации может изменяться вместе с возможностями по слежке в руках распространителя. Чем больше государство знает о своих гражданах, тем больше у него появляется возможностей манипулировать ими.

Степень использования

Степень использования тех или иных методов контроля за информацией, как правило, зависит от местных факторов. В некоторой мере возможности




государства ограничены имеющимся в его распоряжении набором инструментов. По сравнению с Китаем, у России меньше возможностей для строгой онлайн-цензуры из-за менее современной технологической инфраструктуры для мониторинга интернета.¹⁹ Российские власти опираются на устрашение населения (через посадки оппозиционных кандидатов) и манипуляции общественным мнением через пропаганду и дезинформацию. Возможно, Россия опирается на эти методы, потому что они не требуют высоких технологий.

Возможности

Возможности страны по слежке за гражданами определяет количество доступных властям средств контроля информации. Например, страна, использующая шпионское ПО для проникновения в мобильные телефоны, может иметь доступ к информации, позволяющей воздействовать на деятелей оппозиции. Но без технологии глубокого анализа пакетов данных (используемой для фильтрации онлайн-активности и слежки), иная информация остается недоступной, а это ограничивает возможность атаковать других диссидентов. Более мощная слежка не обязательно ведет к более эффективному контролю за информацией, но у правительств, располагающих более сложными технологиями слежки, шире выбор средств информационного контроля. Использование слежки в типологизации контроля за информацией позволяет более обоснованно сравнивать страны. Китай имеет больше возможностей для слежки, чем Россия, поэтому у него больше возможностей внедрения контроля за информацией (подробно об этом в следующей главе доклада). Таким образом, количество и разнообразие инструментов слежки является ключевым фактором для понимания разницы между китайской и российской моделью контроля за информацией.

Слежка, самоцензура, цензура и стратегическое распространение информации вместе составляют механизмы и форму контроля за информацией. Модель информационного контроля зависит от того, какие конкретные механизмы и в



какой степени использует каждая страна и каким количеством инструментов владеет для их внедрения.

В следующих главах иллюстрируется, что для обеспечения внутренней стабильности Россия опирается на повсеместную слежку, самоцензуру и стратегическое распространение информации, в то время как Китай преимущественно использует цензуру и стратегическое распространение информации, подкрепленные обширным наблюдением. Между двумя системами контроля есть и пересечения. Как и в России, в Китае стимулируется самоцензура с помощью регулирования, требующего регистрации на онлайн платформах под настоящими именами, а владельцам VPN грозит тюремное заключение.²⁰ А российская цензура опирается на список заблокированных сайтов, аналогично китайской.²¹

2. КИТАЙСКАЯ И РОССИЙСКАЯ МОДЕЛИ КОНТРОЛЯ ЗА ИНФОРМАЦИЕЙ

При сравнении российской и китайской моделей контроля за информацией, полезно изучить в какой мере каждая из них опирается на различные механизмы, равно как и доступные для их внедрения инструменты.²²

Российский подход

СЛЕЖКА

Закон об оперативно-розыскной деятельности, принятый в 1995 году, заложил правовые основы для всепроникающей системы слежки. Он позволил Федеральной службе безопасности запустить свою технологическую систему для слежки, известную как СОПМ или Систему для оперативно-розыскных мероприятий.²³ СОПМ-1 направлена в первую очередь на перехват звонков по стационарным и мобильным телефонам. СОПМ-2 мониторит интернет-трафик и должна была справиться с растущим уровнем проникновения доступа к сети.

COPM-3 расширила возможности уже работающей системы слежки, добавив функционал мониторинга социальных медиа и Wi-Fi сетей.²⁴

САМОЦЕНЗУРА

В начале 2000-х в России была принята Доктрина информационной безопасности, в которой национальная безопасность напрямую увязывается с информационной безопасностью.²⁵ Далее последовали ограничения: в 2014 году были приняты “закон о блогерах” и закон против шифрования, а в 2016 году был принят закон, требующий хранить данные на территории страны.²⁶ Эти законы были направлены на то, чтобы продемонстрировать растущую слежку и запустить самоцензуру.²⁷

Одновременно российские власти запугивали артистов, журналистов, руководителей технологических компаний и представителей оппозиции. Оппозиционер Борис Немцов был убит, политический активист Алексей Навальный стал регулярным гостем тюрем, а Павел Дуров, основатель VK и мессенджера Telegram, вынужден был бежать из страны после усилившегося давления со стороны властей.²⁸ Более аккуратные меры устрашения имеют долгосрочный эффект. Запускается государственный дискурс об опасности интернета, который должен усилить самоцензуру.²⁹

СТРАТЕГИЧЕСКОЕ РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ

Российская пропаганда и дезинформация фокусируются на распространении сообщений, лояльных действующему режиму.³⁰ Как показывают Галлахер и Фридхайм (Gallacher and Fredheim), Агентство интернет-исследований, российская фабрика троллей, в основном сосредоточено на создании объединяющих сообщений для внутреннего потребления. Сообщения в Твиттере, фокусируются на поддержке вмешательства в Украине и Сирии и подчеркивают разногласия среди западных стран. Российские тролли с большой вероятностью будут

распространять контент государственных медиа, таких, как «Первый канал», «Россия-1», НТВ, «Комсомольская Правда» и «Известия».³¹ Эти действия помогают Кремлю максимально широко донести информацию, распространяемую в стратегических целях. Агентство интернет-исследований платит блогерам, а молодежное движение «Наши», ещё одна организация, распространяющая пропаганду, в большинстве своем состоит из тайно трудоустроенных граждан.³² Некоторые из них работают полный рабочий день, проводя в офисе 12-часовые смены.³³

ЦЕНЗУРА

Долгое время российское правительство уделяло мало внимания цензуре. В отличие от Китая, Россия была неспособна создать внутренние заменители международных медиа-платформ. Российские технологические компании не могли захватить значительную долю рынка, что позволило бы исключить или заменить зарубежных конкурентов. Речь идет о компаниях, которые содержат магазины приложений, поисковые машины или социальные медиа.³⁴ Несмотря на это, Россия фильтрует онлайн. Существует национальный список блокированных сайтов, Россия использует имеющиеся у неё продвинутые возможности для слежки, такие, как технологии глубокого анализа пакетов данных.³⁵ Но все же фильтрация остается менее строгой, чем в Китае. Например, Youtube-канал Алексея Навального остается доступным, несмотря на критическую позицию в адрес Кремля.³⁶

Недавно Россия более решительно взялась за свою онлайн-среду, попытавшись заблокировать мессенджер Telegram, в итоге многие российские ресурсы оказались недоступными из-за грубости предпринимаемых властями методов.³⁷ Telegram остается доступным в магазинах приложений, а российское правительство опозорилось из-за своей неспособности реализовать блокировку. История явно иллюстрирует меньшую способность России к блокировке по сравнению с Китаем, который внедряет цензуру намного более аккуратно и незаметно. Несмотря на поправки по ограничению использования VPN,

принятые в 2017 году, в российских магазинах приложений Apple Store и Google Play Store обильно представлены обходные программы.³⁸

Китайский подход

СЛЕЖКА

По сравнению с Россией, у Китая больше возможностей для надзора за своими гражданами, так как оборудование для слежки используется повсеместно.

Например, в Синьцзяне за гражданами постоянно следят с помощью внедренных приложений, распознающих лица камер и иных технологий.³⁹ Оборудование для слежки широко применяется и в китайской образовательной системе: в классах работает система распознавания лиц, а перемещения учеников контролируются специальными браслетами..⁴⁰ Это наблюдение ведется школами, но получает широкую правительственную поддержку через инициативу «умного образования».

Своими инициативами государство помогает частным акторам в системе слежки подталкивать население к самоцензуре. Частные акторы играют дополняющую роль в китайской слежке. Исследования показывают, что постоянное нахождение под наблюдением может запускать самоцензуру.⁴¹ Мы предполагаем, что такой эффект имеет место в Китае в результате усиленной слежки.

ЦЕНЗУРА

Самый известный пример китайской цензуры — это великий файрвол, ограждающий китайцев от доступа к сервисам гугл, фейсбук и твиттер. Тысячи цензоров в правительстве Китая и в частных компаниях просеивают массу информации для определения новых ключевых слов для блокировки.⁴²

Значительная часть этой цензуры всё еще проводится вручную, но некоторые задачи уже автоматизированы, в том числе блокировка уже известных ключевых слов.⁴³ Снова становится актуальным вопрос, поставленный Рэем Брэдбери в




романе «451 градус по Фаренгейту»: «Вы читали когда-либо книги, которые сжигаете?»⁴⁴ Или, перефразируя: читают ли цензоры цензурируемый ими контент? В будущем, возможно, уже не будут, так как значительная часть этих задач будет автоматизирована благодаря искусственному интеллекту. Недавно Китай усилил цензуру для элит и технологически подкованных граждан, пытающихся получить доступ к зарубежным сайтам. Ряд правовых мер привел к удалению VPN сервисов, не прошедших правительственную проверку, из магазинов приложений, что привело к резкому ограничению доступности VPN в двух крупнейших магазинах приложений — Apple Store и Tencent App Store.

45

СТРАТЕГИЧЕСКОЕ РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ

Как и в России, стратегическое распространение информации играет существенную роль в стратегии правительства Китая по отвлечению внимания граждан от политически острых тем. Целью китайской системы является не участие в спорной теме, а вывод контента в сторону проправительственных постов.⁴⁶ Ещё в 2004 году китайские власти нанимали персонал для влияния на политические мнения в сети.⁴⁷ Они признали, что недостаточно только решать, какая информация будет доступна; следует также формировать информацию, которая будет находиться в сети. Для достижения этой цели тысячам комментаторов ставились задачи по размещению постов. Они получили неофициальное название «Партия 50 центов».⁴⁸ Сегодня, по некоторым оценкам, до двух миллионов подобных сотрудников генерируют около 450 миллионов постов в год.⁴⁹

У российской и китайской систем стратегического распространения информации есть общие черты. Оба режима постят проправительственные сообщения, стараются увести дискуссию от спорных тем и совсем не стремятся поучаствовать в осмысленной политической дискуссии.

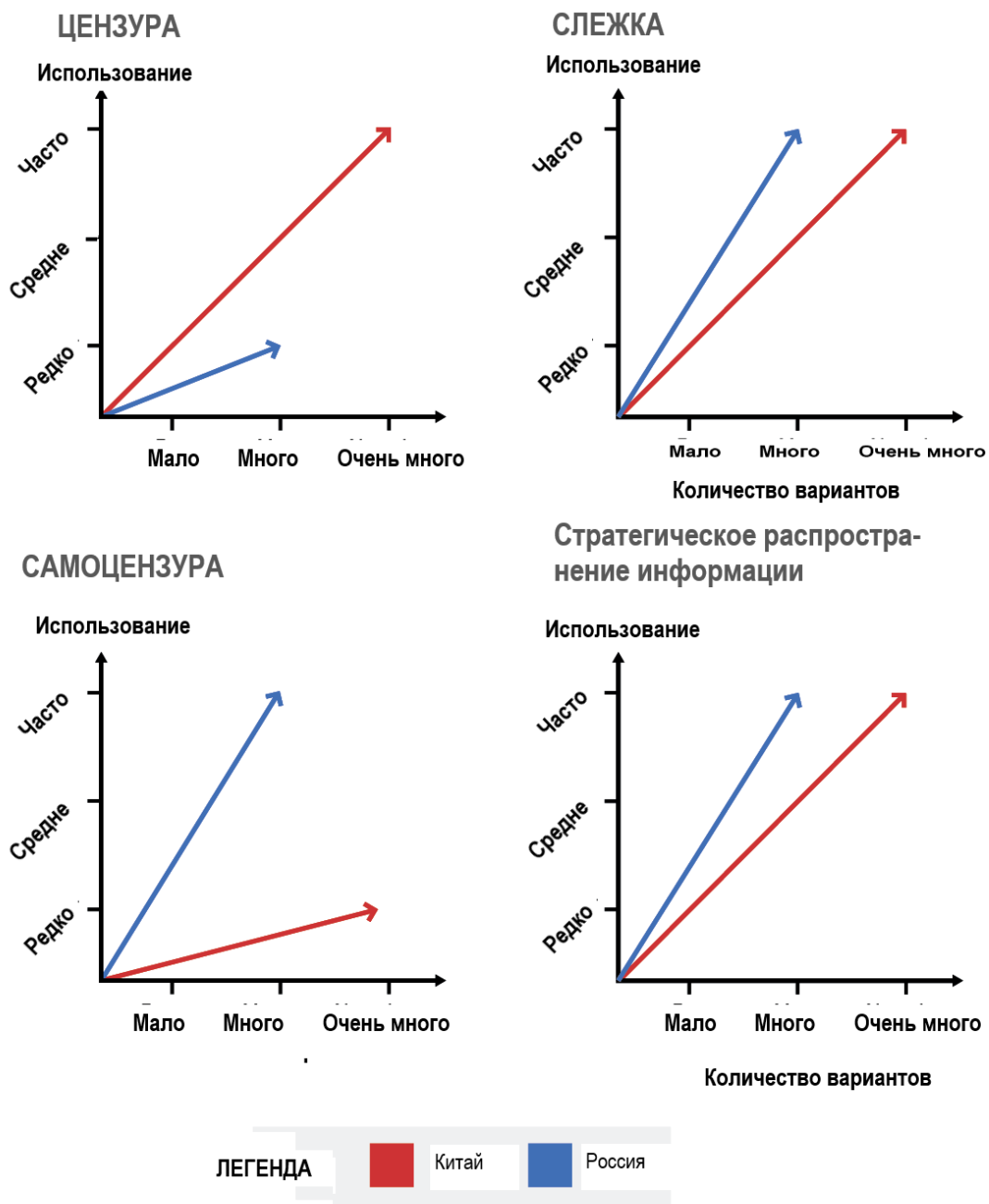


По всей видимости, «партия 50 центов» состоит в основном из государственных служащих, для которых постинг является побочной занятостью. Их дополняют волонтеры, такие, как молодые члены коммунистической партии, которые в рамках Добровольной кампании по цивилизации Интернета бесплатно размещают патриотический контент.⁵⁰

САМОЦЕНзуРА

Запуск самоцензуры с помощью устрашения был широко применяемым методом в Китае времени Мао. С тех пор методы изменились в сторону контроля за информацией, основанного на цензуре и стратегическом распространении информации.⁵¹ Сегодня китайское правительство стимулирует самоцензуру на уровне элит, используя цензуру и распространение стратегической информации в работе с широкими слоями населения (такая стратегия работает лучше со средним гражданином).⁵² Самоцензуру, например, запускает арест человека, предоставлявшего услуги VPN (предостережение для других провайдеров VPN) или введение правила обязательного использования настоящего имени при регистрации в социальных медиа.⁵³ Для дополнительного стимулирования самоцензуры китайские законы зачастую специально оставляют расплывчатыми, чтобы до конца оставалось неясным, что наказуемо и что нет..⁵⁴

Российская и китайская модели контроля за информацией



Графики 1 – 4: Китайская и российская модели контроля за информацией.

3. МЕТОДОЛОГИЯ ИЗМЕРЕНИЯ РАСПРОСТРАНЕНИЯ

В настоящем докладе распространение российских и китайских технологий и методов контроля за информацией исследуется путем сбора информации из открытых источников, в том числе данных, полученных из отчетов компаний, технических измерений, проводимых в сетях, статей в газетах и журналах, законов и нормативных актов, принимаемых государствами.

Распространение измеряется тремя индикаторами: технологии, имитация и обучение. Цель использования этих трех индикаторов — измерить ширину и глубину проникновения российской и китайской тактик в другие страны. Ширину следует понимать как количество стран, которые восприняли хотя бы один индикатор. Глубиной проникновения мы назовем количество индикаторов, принятых отдельной страной. Если страна принимает только один индикатор распространения, мы относим её к периферии техносферы. Если страна принимает максимум индикаторов (два для России, три для Китая),⁵⁵ влияние представляется глубоким, и страна располагается в центре техносферы.

Индикатор 1: технологии

Первый индикатор распространения — технологии. В рамках доклада я сконцентрировал свое внимание на экспорте российских и китайских технологий для слежки и цензуры, которые передаются зарубежным организациям с целью контролировать большое количество людей или общественные здания; предполагается, что они будут использоваться в первую очередь полицией или иными правительственными силами. Примерами такого типа технологий являются камеры, установленные в тюрьмах, портах, городах, железнодорожных станциях, аэропортах, и оборудование для фильтрации, развернутое у зарубежных интернет-провайдеров. Тем не менее, этот индикатор не включает проекты, где предполагается, что полиция или правительство не являются первичными операторами системы слежки, например, поставку компанией

Hikvision камер наблюдения для одного из государственных университетов в Японии.⁵⁶

В дополнение к сбору информации о фактах экспорта технологий слежки с помощью заявлений компаний и сообщений в медиа, я установил наличие некоторых промежуточных устройств, используемых для слежки с помощью сетевых измерений, проведенных совместно с Василисом Верверисом (Vasilis Ververis), Нгуеном Фон Хон (Nguyen Phong Hoang) и Мариусом Исаакидисом (Marios Isaakidis).⁵⁷ Мы использовали инструменты OONI Explorer и Censys, чтобы найти промежуточные устройства Huawei, имеющих отпечаток "V2R2C00-IAE/1.0." Этот отпечаток или заголовок ассоциируется с продукцией eSight от компании Huawei, которая способна анализировать сетевой трафик и определять VPN-сервисы, использующие протокол IpSec, что позволяет использовать их для мониторинга и цензурирования трафика.⁵⁸ Изучение данных OONI Explorer и Censys показало наличие промежуточных устройств Huawei в Колумбии, Италии, Мексике, Нигерии, Пакистане, Турции и на Кубе.⁵⁹

Индикатор 2: имитация

В данном докладе под имитацией мы понимаем воспроизводство третьими странами китайских или российских методов и законов в сфере контроля за информацией. Например, Узбекистан копирует российские законы, касающиеся государственной слежки;⁶⁰ Танзанийские и Зимбабвийские официальные лица сообщают, что они планируют по примеру Китая произвести замену зарубежных контент-провайдеров национальными аналогами для большего контроля.⁶¹ Собранные в докладе данные показывают, что имитация крайне редко (или вовсе никогда) происходит без сопутствующей передачи технологий и обучения, в то время как передача технологий или обучение могут происходить сами по себе. Таким образом, имитация говорит о глубоком влиянии. Стоит отметить, что все страны, имитирующие Россию или Китай, находятся в ядре соответствующей техносферы.

Индикатор 3: обучение

В данный индикатор мы включаем две группы программ: во-первых, это обучение для правоохранительных органов, государственных служащих и частных компаний (которые часто внедряют контроль за информацией в рамках госзаказа); во-вторых, это обучение журналистов. Первую группу обучали тому, как расширить доступ к информации о гражданах (цифровая криминалистика, проекты безопасного города) или тому, как использовать цензуру более эффективно. Все проекты внедрения умного города или продажа технологий глубокого анализа пакетов данных сопровождалась обучением по работе техники. Но в настоящем докладе мы включаем только те случаи, когда в документах явно упоминается, что обучение проводилось для конкретной страны. Новостное сообщение о том, что Huawei внедряет безопасный город в Испании не будет квалифицировано как обучение.

Что касается второй группы, обучение зарубежных журналистов в Китае может оставаться незаметным для правительств, так как некоторые тренинги проводятся частными или новостными организациями. Задачей этих стажировок является улучшение имиджа Китая за рубежом. Как показывают многие примеры, желаемого политического эффекта удастся успешно достичь.⁶²

Термин «обучение» зачастую может быть неправильно понят. В западном мире под ним скорее понимают достижение определенного стандарта, повышение квалификации, проходящее в академическом режиме. В то же время в Китае медиа-тренинги — это скорее бесплатные ознакомительные поездки в Китай, программа которых всегда имеет проправительственную повестку. Подобная стратегия в области СМИ является ключевым элементом китайской стратегии мягкой силы. Так, намерение Китая «обучить» сотни латиноамериканских журналистов в ближайшие годы следует понимать как способ ввести лидеров общественного мнения под действие пропаганды Пекина.⁶³


Более того, тренинги для журналистов часто содержат элемент практического обучения внедрению методов контроля за информацией. Академия высшего руководства в Байсэ (провинция Гуанси), управляемая отделом кадров коммунистической партии Гуанси, яркий тому пример. Официальные лица и журналисты из Юго-Восточной Азии проходят здесь тренинги по «управлению общественным мнением» в сети.⁶⁴

4. ПРИЧИНЫ РАСПРОСТРАНЕНИЯ КОНТРОЛЯ ЗА ИНФОРМАЦИЕЙ

Глава посвящена анализу опыта распространения данных, в ней объясняется, почему отдельные страны охотнее перенимают и покупают технологии, направляют своих представителей на обучение, чем другие. Основываясь на эмпирических данных, представленных в Приложении 1, автор доклада утверждает, что тип политического режима в стране и уровень взаимосвязей между странами объясняет, почему распространение контроля за информацией более вероятно в одних случаях и менее вероятно в других.

Переменная 1: тип политического режима


Тип режима является ключевой переменной для объяснения имитации, но мало влияет на распространение технологий и обучение. В настоящем докладе тип режима определяется в соответствии с Индексом демократии Economist Intelligence Unit, разделяющим страны на демократии, гибридные и авторитарные режимы.⁶⁵ Собранные в исследовании данные показывают, что авторитарные и гибридные режимы с большей вероятностью подражают в своих действиях России и Китаю. Из 19 стран, имитирующих действия Китая и России (в том числе Россия, имитирующая действия Китая, и наоборот), 58% — авторитарные, 37% — гибридные. Всего 5% — демократические государства.



Почему гибридные и авторитарные режимы с большей вероятностью будут имитировать Китай и Россию? Первой причиной представляется то, что авторитарные правительства более склонны учиться друг у друга, так как перед ними стоят схожие угрозы их существованию.⁶⁶ Эта склонность ведет к обмену различными методами и политиками среди автократий. Ещё в 1848 году автократы из разных стран обменивались методами и мнениями о том, как противостоять революционным тенденциям в Европе. Во время Арабской весны в начале 2010-х авторитарные режимы занимались «обучением элит друг у друга», благодаря чему им удалось принять более информированные решения. В некоторых случаях содействие одного авторитарного режима другому может быть достаточно завуалированным, например передача знаний, в других же оно оказывается открытым и прямолинейным. К последним относится помощь по подавлению инакомыслия, оказанная Бахрейну Саудовской Аравией в 2011 году.⁶⁷

Тип режима в меньшей степени объясняет другие индикаторы — технологии и обучения. Хотя авторитарные и гибридные режимы преобладают среди государств, перенявших у Китая и России методы контроля за информацией (56%), они в этом не одиноки. Демократические государства тоже склонны покупать технологии и принимать участие в обучении — они составляют 37% стран, в которые проник контроль за информацией.⁶⁸ Возможно, закупка технологий для слежки воспринимается как нечто более совместимое с демократическими ценностями, так как эти технологии могут быть использованы для вполне «легитимных» целей. Аналогичным образом, участие специалистов в тренингах по цифровой криминалистике или обучение журналистов в Китае не обязательно воспринимается как угроза демократическим ценностям.

Более того, многие из импортируемых технологий имеют двойное назначение. Такие демократические страны, как Аргентина, Бразилия, Германия, Италия или Испания импортировали оборудование для предотвращения уличной




преступности в системе «умных городов».⁶⁹ Но эта же технология может использоваться для пресечения массовых акций протеста.

Как бы мы ни были убеждены, что в демократической стране не будет места злоупотреблению оборудованием для наблюдения, реальный потенциал для этого сохраняется. Развитая технология слежки всегда создает причины для беспокойства. Демократические государства широко используют авторитарные и нелиберальные практики.⁷⁰ Яркими примерами служат США под управлением Дональда Трампа, Венгрия при президенте Викторе Орбане или режим Родриго Дутерте на Филиппинах.⁷¹ Более того, технологии сами по себе не являются непредвзятыми, что оставляет возможность для неумышленных злоупотреблений. Так, Microsoft отклонила запрос калифорнийских правоохранительных органов на предоставление технологий распознавания лиц для портативных нагрудных камер сотрудников полиции и камер патрульных автомобилей. Компания опасалась, что технология может несправедливо использоваться в отношении представителей меньшинств, так как алгоритмы отрабатывались на выборках, состоящих преимущественно из белых мужчин.⁷²

Граждане таких демократических стран, как Австралия, Индонезия, Соединенное Королевство и Соединенные Штаты, участвовали в различных тренингах проводимых китайскими организациями.⁷³ Физические лица из Великобритании участвовали в тренингах Meiya Pico по методам цифровой криминалистики, а журналисты из США и Австралии посещали Китай с образовательными поездками.⁷⁴

Переменная 2: взаимосвязанность

Двухсторонние экономические, политические, исторические и социальные связи между государствами или иными политическими образованиями между могут объяснить почему китайские или российские средства контроля за информацией распространятся больше в одних странах и меньше в других. Чем крепче взаимосвязь между Россией/Китаем и третьей страной, тем вероятнее



распространение там средств контроля над информацией. Данное утверждение схоже, но не совпадает полностью, с концепцией связей Левитского-Вэй (Levitsky and Way), которая опирается на плотность связей между государствами для построения гипотез о распространении в них демократических практик.⁷⁵ В своих работах эти авторы исследуют концепцию связанности на основе сложившихся после Холодной войны отношений между Западом и склонными к авторитаризму режимами и делают вывод: там, где присутствуют более тесные связи, более вероятна демократизация.⁷⁶ Исследователи Амброзио и Вейланд (Ambrosio and Weyland) также размышляли над аргументом о связях и географической близости в контексте распространения авторитаризма.⁷⁷ Основной тезис настоящего доклада сформулирован с учетом результатов вышеупомянутых исследований, тем не менее наши выводы существенно отличаются по ключевым моментам.

Например, Левитский и Вэй утверждают, что самый важный фактор построения связей между странами — географическая близость.⁷⁸ Однако, Китай, например теснее связан с государствами находящимися от него далеко, чем с соседями, во многом благодаря росту своего экономического влияния в мире.

Финансирование проектов за рубежом — хороший пример. Список регионов, которые финансирует Китай возглавляет Африка, следом идут Центральная и Восточная Европа (включая Россию) и Латинская Америка.⁷⁹ И только после этих регионов в списке появляются Южная, Юго-восточная, Центральная и Северо-восточная Азия. Представленные в настоящем докладе данные о контроле за информацией также иллюстрируют этот тренд.

Российские методы контроля за информацией особенно глубоко распространились в странах Содружества независимых государств, но многие страны-реципиенты также не являются соседями России. Китайский опыт контроля за информацией распространился широко и глубоко по миру, отчасти опровергнув гипотезу о географической близости как о самом сильном факторе в установлении взаимосвязей, которые, в свою очередь, влекут за собой распространение средств контроля за информацией.

Левитский и Вэй также утверждают, что наличие рычаги давления «или уровень восприимчивости властей к внешнему давлению, направленному на демократизацию», может объяснять изменение принятых в стране процедур и практик.⁸⁰ Исходя из этого, можно представить, что в процессе распространения средств контроля за информацией демократические государства могут оказывать давление на другие страны, чтобы те не импортировали средства информационного контроля. Но технологии контроля по своей природе имеют двойное назначение — пропагандистский тренинг можно назвать учебной программой для журналистов — и поэтому демократическим сложно критиковать подобный экспорт, избежав при этом обвинений в лицемерии. В конце концов, демократические страны сами по себе являются как крупными экспортерами подобных продуктов, так и слушателями организованных Китаем образовательных программ в области контроля за информацией.⁸¹ Также можно представить, что Китай и Россия задействуют свои рычаги воздействия на страны, чтобы те импортировали средства контроля за информацией, но в рамках предваряющего данный доклад исследований фактов такого воздействия зафиксировано не было. Наконец, данные, представленные в Приложении 1, как раз указывают, что ключевой причиной распространения не является использование внешних рычагов давления — санкций, угроз использования военной силы или отмены финансовой помощи. Более правдоподобным оказался обратный вывод — на подобное оборудование и методы существует активный спрос.

В связи с вышесказанным, в этом докладе предлагается термин «взаимосвязанность» — он позволяет лучше понять причины распространения импортных средств контроля за информацией в тех или иных государствах. «Взаимосвязанность», наряду с типом политического режима — объясняющей переменной, описанной выше, — используется в настоящей работе для оценки вероятности приобретения средств контроля за информацией (см. Таблицу 1).

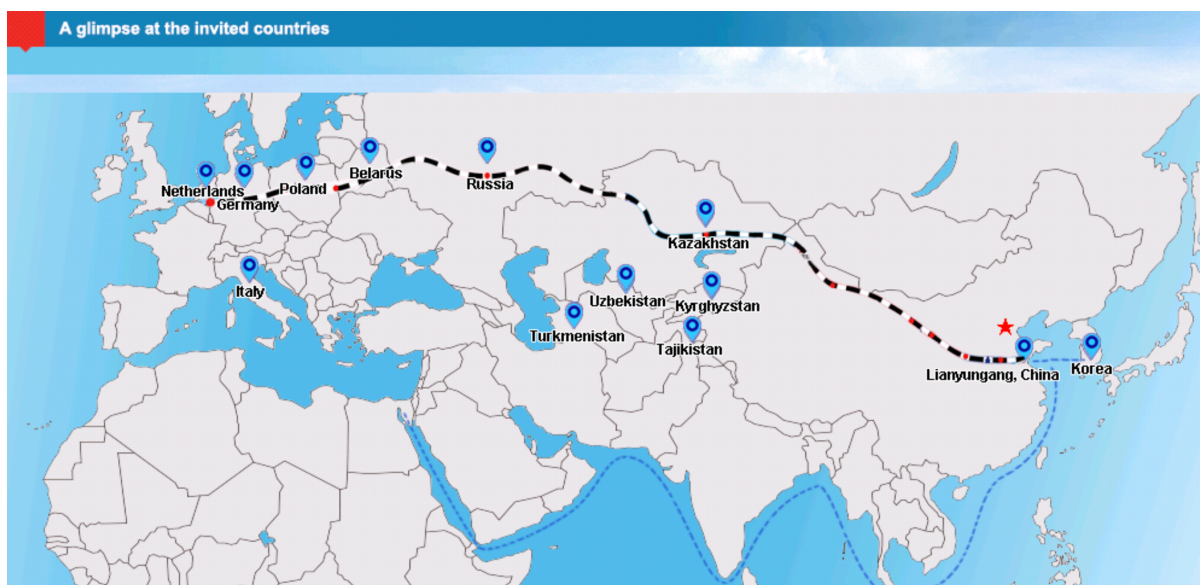
	Россия/Китай	Россия/Китай	Россия/Китай
Объясняющая переменная	Взаимосвязанность	Тип режима / Взаимосвязанность	Взаимосвязанность
Индикаторы проникновения	Фильтрация или технологии слежки	Имитация законов и методов	Обучение официальных лиц и представителей правоохранительных органов; журналистов и сотрудников частных компаний
Широта и глубина проникновения Страна X K(1), P(2)	Ширина "Страна X" и глубина "K(1) P(2)" проникновения указаны в левой части таблицы		

Таблица 1: Измерение распространения.

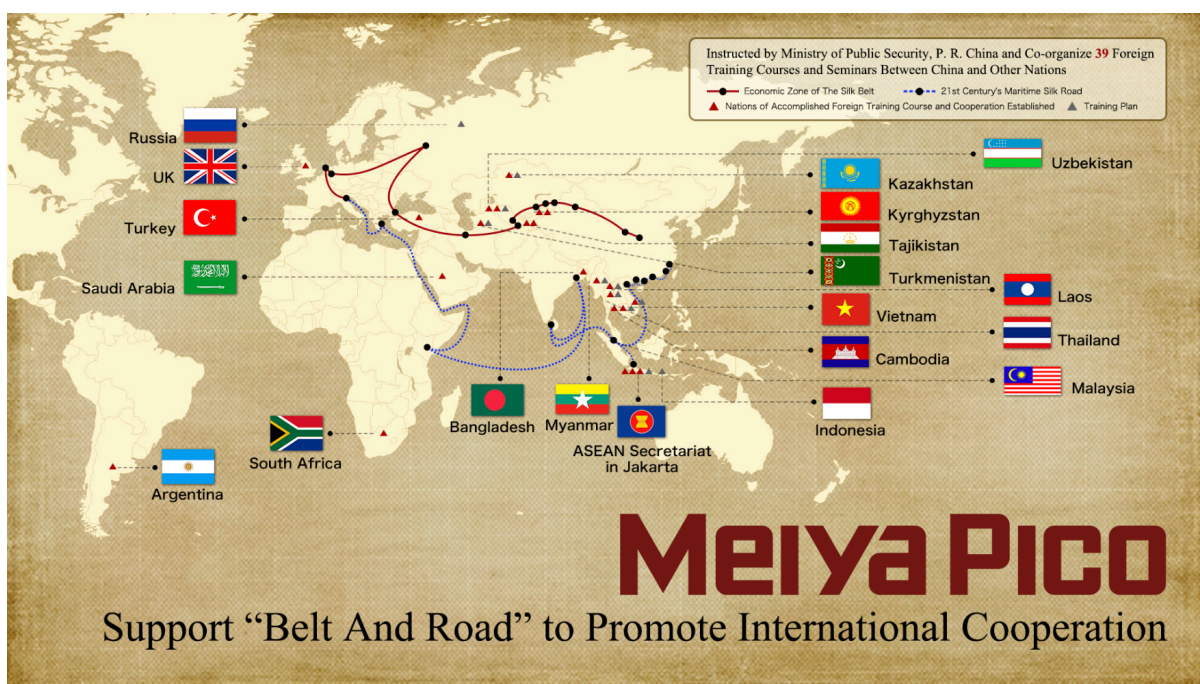
ПОСРЕДНИКИ ВЗАИМОСВЯЗЕЙ

В настоящем докладе инициатива «Один пояс — один путь» и Содружество независимых государств воспринимаются как один из способов демонстрации тесной связи с Китаем или Россией. Страны, входящие в инициативу, в содружество или в обе структуры, с большей вероятностью используют российские или китайские средства контроля за информацией. Это объясняется тем, что упомянутая инициатива и СНГ являются ключевыми проводниками существенных экономических, дипломатических, технократических, информационных связей, связей гражданского общества между Китаем или Россией с одной стороны и третьей страной с другой. Множество факторов

подтверждают эту схему. Во-первых, обе структуры возвращают нас к историческим нарративам, которые предполагают тесные взаимосвязи между Китаем/Россией и иной страной. «Один пояс — один путь» основан на идее воссоздания древнего Шелкового пути.⁸² СНГ основан на традиции бывшего СССР и действует для сохранения этих связей. Во-вторых, обе инициативы опираются на активную поддержку России или Китая. Россия часто вмешивается в ситуацию в Восточной Европе или Центральной Азии — регионах, которые она считает частью своей сферы влияния; а Китай поддерживает обмен идеями, товарами и социальное взаимодействие в рамках инициативы (это взаимодействие формально закреплено в двухсторонних меморандумах о взаимопонимании).⁸³ Китай вплетает тренинги для журналистов и медиа в свою деятельность в рамках инициативы,⁸⁴ в её же рамках происходит продажа технологий и услуг. С одной стороны, в поисках прибыли китайские компании ищут новые рынки сбыта; с другой, внешняя торговля в определенной мере координируется правительством. Meiyu Pico, китайская компания в сфере кибербезопасности, получает задания от китайского министерства общественной безопасности по проведению тренингов по цифровой криминалистике для стран, включенных в инициативу «Один пояс — один путь» (см. изображение 2). Также Meiyu Pico может принять участие в создании коридора безопасности из Китая в Европу, задачей которого является привязка услуг и продуктов по безопасности к международным проектам развития.⁸⁵ На данный момент предполагается, что в коридор безопасности войдут Казахстан, Россия, Беларусь, Польша, Германия и Нидерланды.⁸⁶



Изображение 1: Иллюстрация планируемого стратегического коридора безопасности, сохраненная с сайта Meiya Pico 1 мая 2019 года.⁸⁷



Изображение 2: Meiya Pico получила указания от китайского министерства общественной безопасности провести тренинги по цифровой криминалистике в странах инициативы “Один пояс - один путь”. На данном изображении, полученном 29 апреля 2019 г., указано 19 стран.⁸⁸




Изображение 3: На этом изображении, полученном 5 сентября 2019 г., указано 29 стран. Meiya Pico удалила упоминание Министерства общественной безопасности (см. Изображение 2) в верхнем правом углу.⁸⁹

5. ЯДРО ТЕХНОСФЕР ПЕКИНА И МОСКВЫ

В настоящем разделе описывается, каким образом высокий уровень взаимосвязанности приводит к широкому распространению методов контроля за информацией и возникновению ядра техносферы. Страны, которые в меньшей степени взаимосвязаны с Россией и Китаем и не входят в «Один пояс – один путь» или в Содружество независимых государств, с меньшей вероятностью будут сталкиваться с широким распространением средств контроля информации. Эти страны остаются на периферии техносфер России и Китая.

Содружество независимых государств (СНГ)

СНГ был образован после распада СССР в декабре 1991 г., его создание должно было способствовать дальнейшему политическому, экономическому и



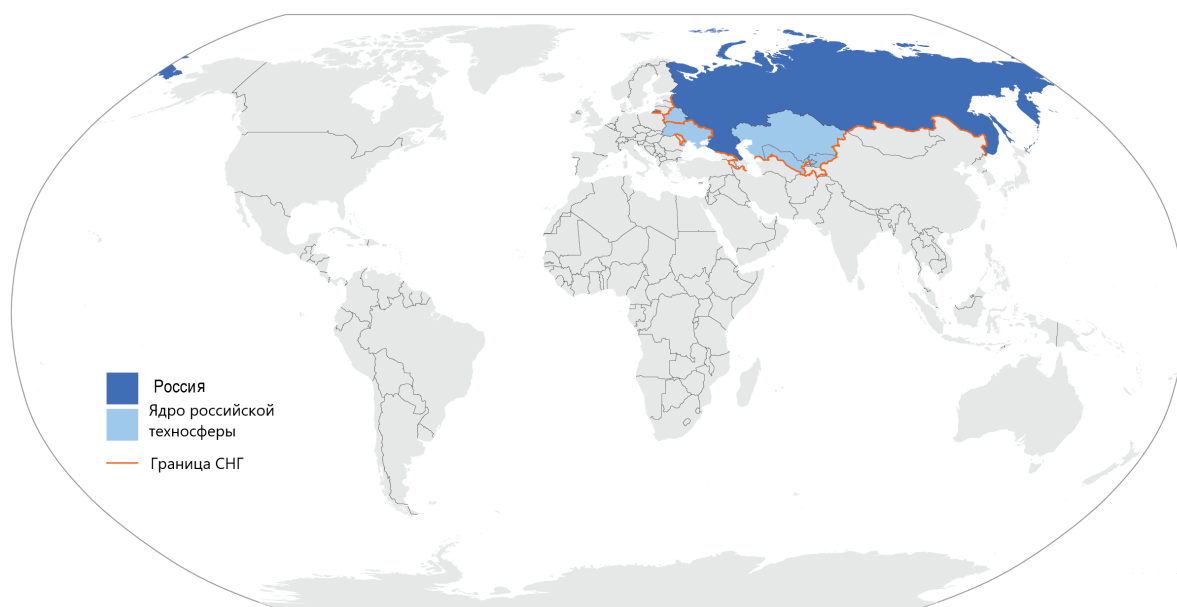
культурному сотрудничеству между РФ и вновь образованными государствами. В СНГ, помимо РФ, входят Армения, Азербайджан, Беларусь, Казахстан, Киргизия, Молдавия, Таджикистан и Узбекистан. Украина, изначально входила в состав СНГ, но покинула организацию в 2018 г.⁹⁰

По результатам исследований, проводившихся при подготовке настоящего доклада, было обнаружено, что российские средства контроля информации распространяются на 28 стран, с разнообразным географическим положением — среди них, например, Мексика и Палестина. В страны СНГ, а также в вышедшую из организации Украину, уходит 25% экспорта российских средств контроля информации (7 стран из 28).⁹¹ Азербайджан, Беларусь, Казахстан, Киргизия, Украина и Узбекистан находятся в центре российской техносферы. В каждой из этих стран в определенное время принимались законы об онлайн-слежке, идентичные российским. Законы о слежке в странах СНГ можно толковать по-разному, но они все оставляют возможности для преследования диссидентов, что по сути копирует российский подход к контролю информации. Однако законодательство и атмосфера страха не были бы столь действенными без наличия технологий слежения, предоставляемых Россией.

МВД Беларуси приобрело технологии российской компании Аналитические бизнес-решения (Analytical Business Solutions), специализирующейся на повышении эффективности мониторинга интернета.⁹² Власти Беларуси приняли законы, аналогичные российским, и по всей вероятности приобрели в России оборудование для слежки СОПМ.⁹³ Казахстан приобрел технологию глубокого анализа пакетов данных у компании VAS Experts, штаб-квартира которой находится в Санкт-Петербурге.⁹⁴ Также он приобрел средства мониторинга от компании iTesco, технологии СОПМ от компаний МФИ Софт (MFI-Soft) и «Протей», средства анализа аудио у компании Центр речевых технологий (Speech Technology Center) и средства анализа мобильных устройств у компании Oxygen Software.⁹⁵ МЧС Казахстана также приобрело Semantic Archive — платформу для анализа информации, поставщиком которой

является Аналитические бизнес-решения (Analytical Business Solutions).⁹⁶ Киргизия приобрела оборудование COPM компаний Oniks-Line и Signatek.⁹⁷ Украина также приобрела оборудование COPM.⁹⁸ Узбекистан импортировал технологии глубокого анализа пакетов данных компаний VAS Experts и Протей, оборудование COPM компании МФИ Софт, средства анализа аудио Центра речевых технологий, и средства анализа мобильных устройств компании Oxygen Software.⁹⁹ Власти Узбекистана также приняли закон о слежке в интернете во многом скопированный с аналогичного российского закона.¹⁰⁰


Ядро российской техносферы вписывается в границы СНГ



Карта 2: Ядро российской техносферы вписывается в границы СНГ.

Проект «Один пояс — один путь»

Проект «Один пояс — один путь» был официально запущен в 2013 г. и охватывает 138 стран: 82% экспорта китайских средств контроля информации идет в страны «Одного пояса» (84 страны из 102).¹⁰¹ Проект включает в себя экономический пояс «Шелковый путь» и «Морской шелковый путь 21-го в.», который призван возобновить использование старых морских торговых путей.¹⁰² Сухопутный и



морской торговые пути дополняет «Цифровой шелковый путь», который должен связать Китай с другими странами за счет сотрудничества в цифровой сфере.


В данном разделе доклада рассматриваются десять стран, входящих в «Один пояс — один путь», в которых особенно массово распространены средства контроля информации (на основе трех критериев распространения). Эти страны входят в ядро техносферы Китая.

Влияние Китая очень сильно в Египте, где применяются китайские технологии наблюдения. Компания Huawei построила в стране безопасный город, а Hikvision поставляет технологии видеонаблюдения для парка автобусов мухафазы Суэц.¹⁰³ Кроме того, группа журналистов из Египта в течение 10 месяцев проходила обучение в Китае по грантам Ассоциации общественной дипломатии Китая. Они могли ознакомиться с авторитарной медиа-средой в Китае благодаря визитам в такие издания, как People's Daily.¹⁰⁴ Египетские функционеры, в свою очередь, были приглашены в компанию Meiya Pico, где могли ознакомиться со средствами цифрового расследования.¹⁰⁵ Египет и Китай сотрудничают в сфере контроля за информацией и на государственном уровне: в 2014 году страны подписали договор о борьбе с киберпреступностью.¹⁰⁶ Четырьмя годами позже в Египте был принят закон о киберпреступности, позволяющий регулировать социальные сети, он использует тот же подход, что применяет Китай в области регулирования социальных медиа-платформ.¹⁰⁷

Иран также подвергся сильному влиянию Китая в области практик контроля информации. Одним из первых был подписан контракт по продаже Ирану компанией Huawei оборудования для наблюдения и слежки, позволяющего государственным органам получать доступ к мобильным телефонам.¹⁰⁸ Еще одна китайская компания, ZTE, продавала Ирану оборудование для перехвата телефонных переговоров граждан.¹⁰⁹ Технологическое сотрудничество было укреплено встречей между представителями государственных органов Китая и Ирана, итогом которой стала договоренность об участии Пекина в реализации

Национальной Информационной Сети Ирана.¹¹⁰ Также Иран активно изучал китайские технологии. По примеру Китая, где существует собственная экосистема приложений, к которой у властей есть доступ, в Иране было разработано приложение «Соруш» для обмена сообщениями.¹¹¹ Глава иранской Организации информационных технологий восхищался Китаем и его «четырьмя десятилетиями положительного опыта в разработке приложений для сервиса в области информационных технологий», отмечая, что в Иране надеются «воспользоваться этим опытом».¹¹²

Малайзия — еще одна страна, расположенная в ядре китайской техносферы. Журналисты из Малайзии обучались в Пекине при содействии МИД Китая, Министерства образования Китая и государственной корпорации «Хуанэн Индастри» (Huaneng Industry).¹¹³ По словам одного из преподавателей Университета Коммуникаций Китая, подобный опыт «может служить основой для развития стажерами медиаиндустрии в родной стране».¹¹⁴ Учебные программы охватывают не только журналистов. «MeiYa Pico», компания из Сямыня, специализирующаяся на кибербезопасности, проводила в Малайзии тренинги по средствам цифровой экспертизы, позволяющим извлечь данные из телефонов и компьютеров. При этом компания заявляла, что, «как и всегда, MeiYa Pico придерживалась стратегии выхода на глобальные рынки и на рынки стран «Пояса и Пути»».¹¹⁵ Малайзия активно покупала технологии наблюдения китайского происхождения. В частности, власти страны приобрели у шанхайской компании Yitu нагрудные камеры для сотрудников правоохранительных органов.¹¹⁶ Помимо этого, они приобрели у Alibaba Group систему управления дорожным движением с возможностью подключения искусственного интеллекта.¹¹⁷ По всей видимости, власти Индонезии намерены и далее двигаться в том же направлении: премьер-министр Махатхир бин Мохамад недавно заявил, что его страна будет использовать, насколько это возможно, оборудование Huawei.¹¹⁸ А бывший заместитель премьера Ахмад Захид Хамиди заявил, что китайская практика продвинутого использования оборудования для слежки с целью мониторинга всех передвижений достойна того, чтобы ее перенять.¹¹⁹




Россия, со своей стороны, активно копировала более сложные методы, применяемые Китаем для фильтрации контента в интернете.¹²⁰ Фильтрация определенного контента, а не целых вебсайтов сокращает риск излишних блокировок. С целью укрепления сотрудничества в Россию пригласили создателей «Великого китайского фаервола» для обмена опытом.¹²¹ Также Россия получила от Китая содействие в области обучения и передачи технологий. Специалисты из России проходили подготовку по цифровой экспертизе в компании Meiya Pico.¹²² Решения Huawei для безопасного города были внедрены в Санкт-Петербурге;¹²³ компания Huawei реализовала решение для облачного хранилища, «специально разработанное для хранения и анализа крупных массивов видеоданных».¹²⁴

Танзания является примером практически линейного распространения контроля информации: сначала передача технологий и обучение персонала, а затем создание местной версии подобных систем. В 2014 г. компания Huawei объявила, что реализовала проект «безопасного города» в Танзании.¹²⁵ Год спустя компания Dahua Technology из Ханчжоу оборудовала Администрацию президента на Занзибаре умными камерами с функцией распознавания лиц и звука.¹²⁶ Еще год спустя People's Daily сообщила, что журналисты из Танзании приняли участие в программе обучения для журналистов, спонсированной Ассоциацией общественной дипломатии Китая.¹²⁷ В свою очередь, укрепление связей между Танзией и Китаем привело к тому, что власти Танзании занялись копированием китайской концепции цензуры. Бывший заместитель министра Транспорта и Коммуникаций Танзании Эдвин Нгояни на двустороннем китайско-танзанийском круглом столе по новым медиа, организованном правительством Танзании и Администрацией киберпространства Китая, заявил: «Наши китайские друзья сумели заблокировать подобные медиа у себя в стране, заменив их сайтами собственной разработки, безопасными, конструктивными и популярными. Мы еще не достигли этой стадии, но, хотя мы продолжаем

пользоваться подобными платформами, нам следует опасаться злоупотреблений в их использовании». ¹²⁸

Таиланд - еще один пример успешного экспорта технологий наблюдения и слежки из Китая. Hikvision взяла на себя задачу обеспечить системами видеомониторинга Министерство торговли Таиланда, ¹²⁹ а также поставляет полиции Таиланда портативные камеры для мониторинга и записи в реальном времени, в том числе удаленного. ¹³⁰ Кроме того, компания Huawei совместно с полицией Таиланда реализует решение для наблюдения eLTE Trunking Joint Innovation Project. ¹³¹ Как и в случае с другими странами «Пояса и пути», компания Meiya Pico обучила тайских экспертов технологиям исследования мобильных устройств и компьютеров, а журналисты из Таиланда приглашались в Китай на стажировки для медиа. ¹³² Бангкок также сообщал о своих намерениях создания «Великого фаервола» по образцу китайского. ¹³³ Хотя изначальный план создания единого интернет-шлюза был отменен, в стране недавно вступил в силу закон, имитирующий китайский закон о кибербезопасности 2017 г. Его такие же расплывчатые формулировки и широкий охват позволяют властям Таиланда проводить обыски в помещениях частных лиц и компаний. ¹³⁴

Уганда также активно сотрудничает с Китаем в области контроля информации. В 2017 году чиновники из Уганды приезжали в Пекин на встречу с Государственной корпорацией Китая по импорту-экспорту электроники (China National Electronics Import & Export Corporation, CEIEC). Стороны договорились, что CEIEC поможет Уганде вести мониторинг социальных сетей, а также предоставит услуги для борьбы с «киберпреступностью». ¹³⁵ В том же году журналисты из Уганды приняли участие в десятимесячной стажировке в Китайско-африканском пресс-центре в Пекине, организованной Ассоциацией общественной дипломатии Китая. ¹³⁶ Год спустя Huawei поставила 900 камер наружного наблюдения для программы умного полицейского наблюдения правительства Уганды. ¹³⁷ Компания из Шэньчжэня также помогала властям Уганды получить доступ к зашифрованным коммуникациям известных оппозиционеров. ¹³⁸ Наконец, в июне 2019 года



Комиссия Уганды по коммуникациям обнародовала проект регламентации интернета, который предполагает централизованный контроль за входящими и исходящими потоками информации в стране. Эта инициатива во многом похожа на попытки Таиланда создать единый интернет-шлюз для всех международных коммуникаций. Согласно источнику в государственных органах Уганды, участвовавшему в регуляторном процессе, «эффектом будет превращение интернета в Уганде в что-то похожее на интернет в Китае, который контролируется централизованно и в основе которого лежит единая система, позволяющая контролировать все».¹³⁹

Тесные взаимосвязи между Замбией и Китаем свидетельствуют о том, что это африканское государство также находится в ядре техносферы Китая. Для осуществления контроля за собственным населением, власти Замбии опираются на цензуру и на оборудование для слежки, поставляемое компаниями Huawei и ZTE.¹⁴⁰ По некоторым сведениям, сотрудники Huawei помогали властям Замбии перехватывать цифровые коммуникации журналистов и членов оппозиции.¹⁴¹ Huawei также реализовала проект умного города в стране, увеличивающий возможности Замбии по физическому наблюдению.¹⁴² Кроме того, сильное влияние на информационную среду Замбии оказали местные журналисты, проходившие стажировки в Китае.¹⁴³ По словам одного из министров Замбии, страна теперь следует «Китайскому пути» в области управления интернетом.¹⁴⁴

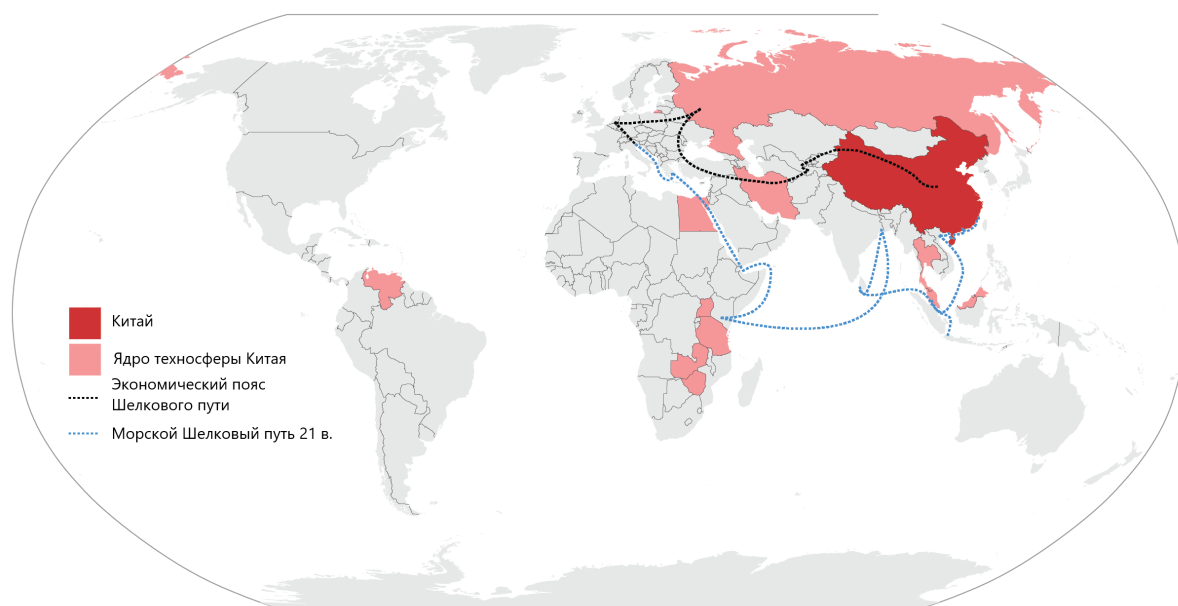
Южный сосед Замбии, Зимбабве, в течение длительного времени сотрудничал с Китаем в области контроля информации. Согласно ряду источников, еще в 2005 г. Китай вел с Зимбабве переговоры о продаже оборудования для перехвата коммуникаций, и уже тогда страна приобрела и использовала китайское оборудование для глушения радиопередач.¹⁴⁵ Это один из первых примеров экспорта Китаем технологий для цензуры, которые со временем были значительно усовершенствованы. Помимо оборудования для блокировки радиотрансляций, китайские компании предоставили властям Зимбабве оборудование для наблюдения. Компания Hikvision из Ханчжоу совместно с

местной компанией Nations Hardware and Electrical проводила проект по внедрению систем видеонаблюдения в стране.¹⁴⁶ Также компания Cloudwalk Technology Co. поставляет камеры с функцией распознавания лиц, которыми могут быть оборудованы железнодорожные станции и аэропорты, в привязке к национальной базе фотографий.¹⁴⁷ Как минимум с 2011 года журналистов из Зимбабве обучали приемам распространения информации (ведение дискуссий, управление СМИ в авторитарической среде).¹⁴⁸ Зимбабве имитировало китайский подход, и власти об этом вполне открыто говорили. В Зимбабве разрабатывались местные приложения-эквиваленты социальных платформ, чтобы обеспечить властям более эффективный контроль.¹⁴⁹ В 2016 г. Супа Мандиванзира, бывший министр информационных и коммуникационных технологий Зимбабве, заявил: «Президент [Мугабе] говорит, что с этим надо что-то делать, и мы делаем. Он ссылался на пример Китая, который очень много сделал для того, чтобы обеспечить надежность интернета».¹⁵⁰

Венесуэла является членом «Пояса и пути» и одной из стран техносферы Китая, хотя расположена в стороне от морских или сухопутных путей проекта. Укрепление связей между Китаем и Венесуэлой началось при правлении президентов Ху Цзиньтао и Уго Чавеса незадолго до мирового финансового кризиса 2008 г.¹⁵¹ Активизация сотрудничества между двумя странами отразилась и на взаимодействии Пекина и Каракаса в области систем наблюдения и слежки. В 2008 г. группа функционеров Министерства юстиции Венесуэлы посетила Шэньчжэнь, где изучала систему карт-удостоверений личности, используемых в Китае.¹⁵² Венесуэльские власти посчитали, что проект достоин повторения. Примерно десять лет спустя в Венесуэле был запущен проект по внедрению идентификационных смарт-карт, известных также под названием «карточка Родины» (*carnet de la patria*), в котором принимала участие компания ZTE из Шэньчжэня. Карта содержит довольно большой массив информации о ее владельце: помимо даты рождения и информации о родственниках, на нее может быть занесена медицинская история, сведения о деятельности в социальных сетях, членстве в политических партиях и участии или неучастии в выборах.¹⁵³

Внесение этих сведений на карту предназначено для стимулирования у ее владельца модели поведения добропорядочного гражданина. Иными словами, китайская система социального кредита, опирающаяся на «сбор и анализ больших данных для наблюдения, влияния и оценки поведения за счет экономических и социальных процессов», более не ограничивается Китаем.¹⁵⁴ Однако сотрудничество между двумя странами в области слежки пошло еще дальше. В стремлении укрепить контроль над населением власти Венесуэлы реализовали в стране ряд проектов «умных городов», а также установили тысячи камер наружного наблюдения производства Huawei, ZTE, и CEIEC.¹⁵⁵ В рамках этого заказа Huawei провела стажировки по эксплуатации этих систем для венесуэльских специалистов.¹⁵⁶

Ядро техносферы Китая расположено вдоль торговых путей «Пояса и Пути»



Карта 3: Ядро техносферы Китая расположен вдоль торговых путей «Пояса и Пути».

Пересечение техносфер

Техносферы Китая и России пересекаются в 20 странах. Интересно, что страны, находящиеся в ядре российской техносферы, частично находятся и в техносфере

Китая. Китай ведет активную деятельность в Беларуси, Казахстане, Киргизии, Украине и Узбекистане. Россия же присутствует только в одной из стран, находящихся в техносфере Китая — Таиланде, куда поставляет оборудование российская компания Центр речевых технологий, специализирующаяся на анализе аудио.¹⁵⁷

6. ВЛИЯНИЕ РАСПРОСТРАНЕНИЯ ТЕХНОЛОГИЙ


Основной результат распространения технологий, о котором идет речь в настоящем докладе — возникновение географической зоны, в которой экспортер средств контроля информации наделен определенным преимуществом. Можно выделить следующие категории преимущества: политические, экономические и разведывательные. В политическом плане распространение технологий контроля информации способствует укреплению авторитарных режимов.¹⁵⁸ Например, широкое распространение за рубежом российского подхода к информационной безопасности полезно Кремлю и во внутренней политике, так как подтверждает легитимность подобного подхода — всегда можно указать на тот факт, что модель была перенята другими государствами. Кроме того, распространение систем контроля информации в других странах закрепляет за страной происхождения систем имидж законодателя стандартов. Обучение иностранных чиновников и журналистов на стажировках позволяет привить политическим лидерам и крупным медиа-игрокам китайское видение того, как должен выглядеть информационный ландшафт в авторитарном государстве. Можно поставить под сомнение действенность обучения небольшого количества функционеров и журналистов из каждой отдельно взятой страны, однако обучение нескольких тысяч людей из самых разных стран мира может привести к более широким структурным изменениям, поставив отдельные страны в зависимость от китайских технологий. Академия информационной безопасности компании Meiyu Pico уже обучила исследованию цифрового оборудования более 1000 сотрудников правоохранительных органов из разных стран мира, а по прогнозам Ассоциации общественной дипломатии Китая, через ее

образовательные программы к концу 2020 года пройдет 1500 иностранных журналистов.¹⁵⁹



Фото 4: Академия высшего руководства в Байсэ (Baise Executive Leadership Academy), где журналисты и чиновники из стран Юго-Восточной Азии обучаются китайским методам контроля информации.¹⁶⁰

В экономическом, плане распространение средств контроля информации создает новые рынки для стран-экспортеров. В Китае и в России в этой области возникло некое подобие военно-промышленного комплекса. В этот «безопасностно-промышленный комплекс» входят политики, зависящие от отраслей связанных с безопасностью, частные охранные предприятия, полиция. Все эти организации и ответственные лица в них получают выгоду от увеличения расходов на безопасность в собственной стране и от экспорта решений за рубеж. Контроль информации — источник доходов для таких компаний, как Hikvision, Huawei, НТЦ Протей, VAS Experts и других производителей оборудования для наблюдения и цензуры из Китая и России. Экспорт технологий контроля информации способствует взаимовыгодному сотрудничеству с покупателями, в особенности для Китая. В частности, Эквадор поставляет в Китай нефть в обмен на поставки



средств слежки и наблюдения. Эти поставки, в свою очередь, создают новые рабочие места и дополнительные доходы в Китае.¹⁶¹

Распространение средств контроля информации с образованием техносферы также имеет последствия для разведки. Например, китайские компании строили штаб-квартиру Африканского Союза в Аддис-Абебе, Эфиопия, после чего Китай подозревали в пересылке значительных объемов данных с установленных в этом здании компьютерных систем в Пекин.¹⁶² Китай же мог использовать полученные данные для того чтобы увеличить эффективность своей внешней политики на континенте. В Пакистане на камерах наблюдения производства Huawei были обнаружены неизвестные Wi-Fi модули. Эти модули могли грозить риском хищения информации, что подчеркивает разведывательное преимущество государства, являющегося экспортером средств наблюдения и слежки.¹⁶³ Также следует отметить, что не только Китай стремится сохранить доступ к поставляемому оборудованию. Российские компании, поставлявшие средства наблюдения в Киргизию, столкнулись с обвинениями в том, что они оставили закладки в установленных системах, что могло позволить им получить доступ к информации.¹⁶⁴

СФЕРЫ ВЛИЯНИЯ В ВИДЕ КОНЦЕНТРИЧЕСКИХ КРУГОВ

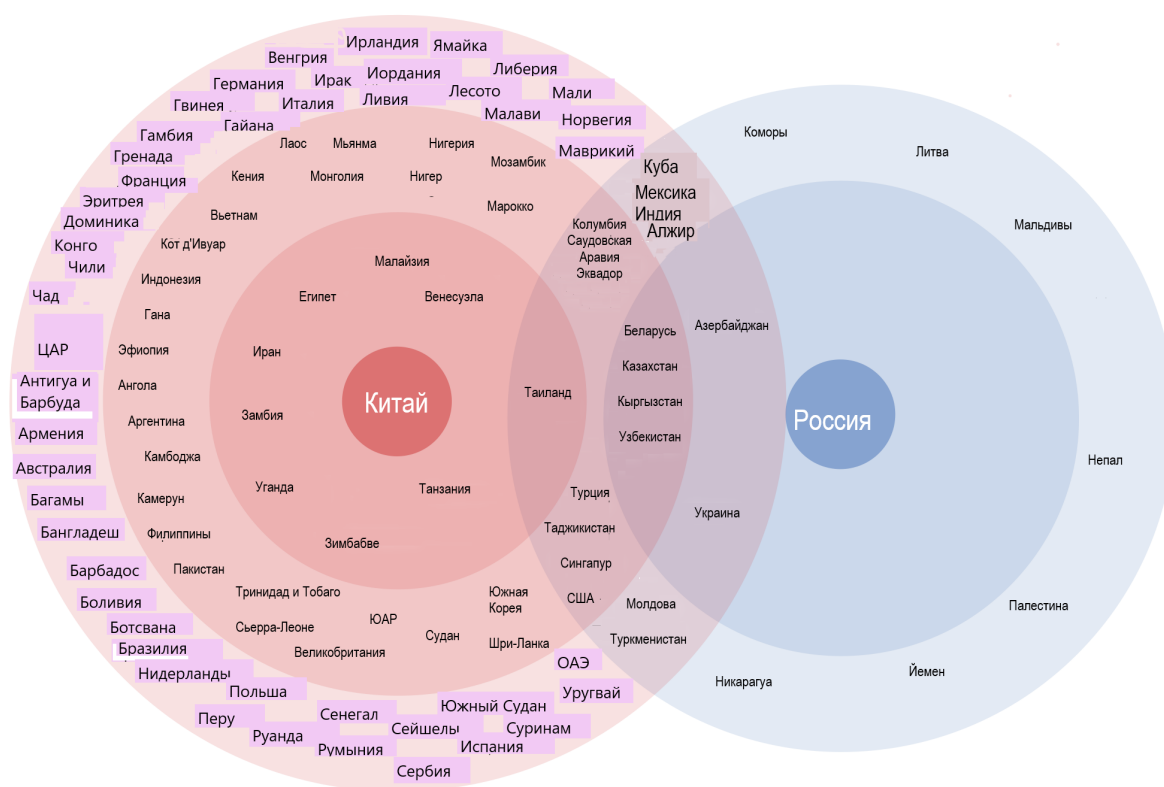
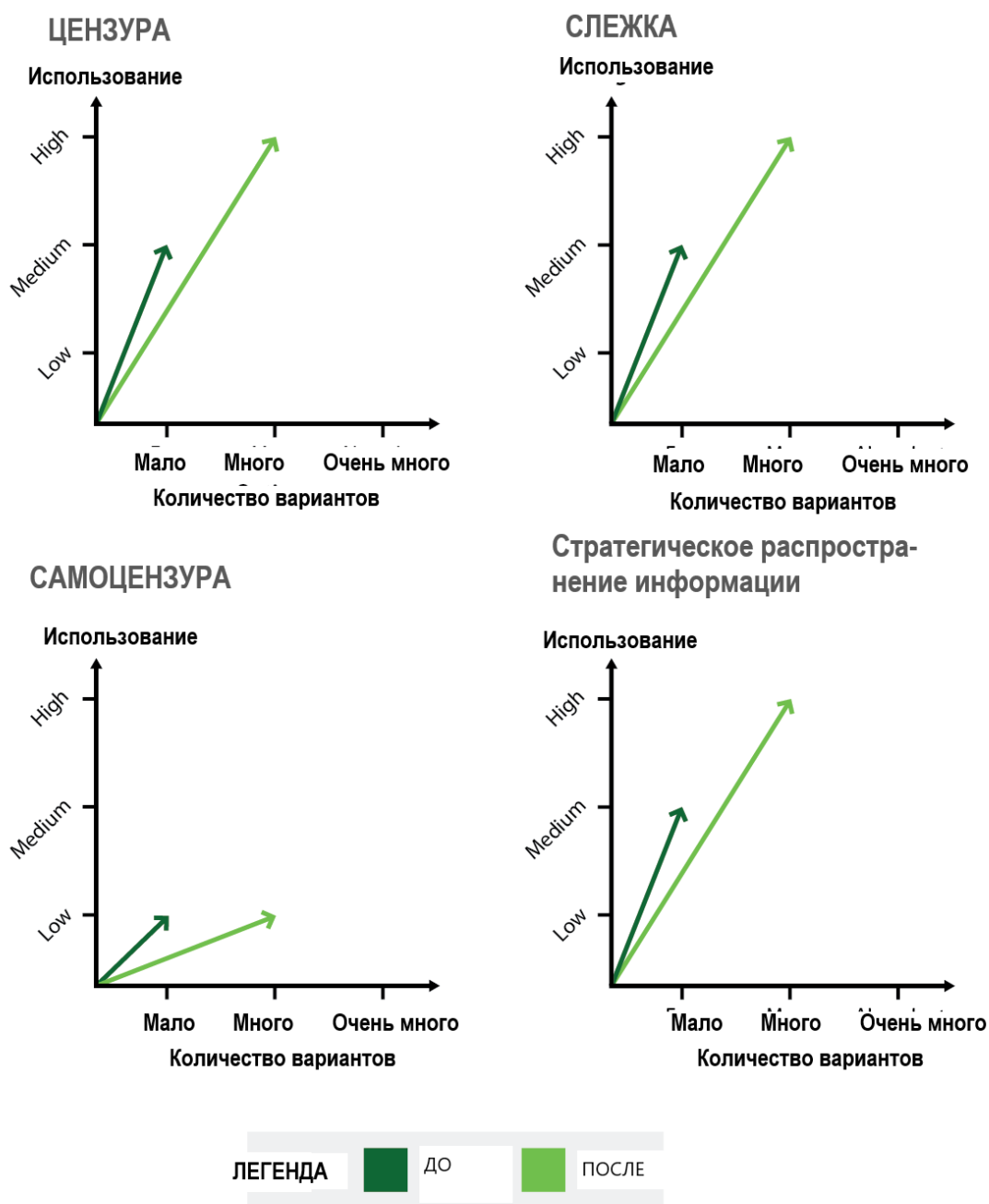


Схема 1: Концентрические круги влияния. Внутренний круг представляет собой ядро техносферы, наружные круги – ее периферию.

Рост распространения технологий влияет на то, каким образом средства контроля информации разворачиваются и эксплуатируются в различных странах мира. На примере Зимбабве видно, что технологии для цензуры и слежки, а также обучение методам пропаганды являются основными статьями китайского экспорта в Зимбабве. Властям Зимбабве распространение этих технологий позволяет эффективнее запугивать население, а также увеличивает его возможности в области цензуры и манипуляции общественным мнением. Иными словами, рост китайского экспорта ведет к росту числа *вариантов* контроля информации в распоряжении Зимбабве. Использование методов контроля за информацией во многом меняется по мере внедрения этих технологий. Возможно, Зимбабве и так опиралось на цензуру и распространение стратегически выгодной информации, но взаимодействие с Китаем привело к

тому, что это африканское государство реализует подобный подход в полном объеме. Сближение подходов к управлению информацией в Зимбабве с китайской моделью подтверждается заявлениями властей африканской страны о намерении воспроизвести у себя дома опыт Китая.

Зимбабве до и после распространения китайских средств контроля информации




Графики 5 – 8: Влияние распространения методов и технологий на ситуацию в Зимбабве. Подробное исследование положения с контролем информации в Зимбабве выходит за рамки настоящего доклада. В связи с этим графики, описывающие ситуацию до и после распространения китайских средств контроля информации, являются гипотетическими. Утверждение о сближении используемых подходов с китайской моделью, однако, гипотетическим не является, и основано на сведениях, собранных в настоящем докладе.

ЗАКЛЮЧЕНИЕ

В настоящем докладе описывается примерно тринадцатилетний период экспорта Китаем и Россией средств контроля информации. За это время значительно изменились характеристики распространяемых технологий. Изначально за рубеж поставлялись преимущественно средства грубой цензуры и слежки. Сюда можно отнести экспорт Китаем оборудования для глушения радиопередач в Зимбабве и экспорт российского оборудования для фильтрации и анализа аудио в страны бывшего СССР. Впоследствии же экспорт был диверсифицирован, а экспортируемые средства усовершенствованы. Сегодня мы можем наблюдать массовые поставки камер видеонаблюдения с технологией распознавания лиц, огромный ассортимент средств исследования цифрового оборудования, удостоверений личности в формате смарт-карт, умных баз данных для властей, технологий умного города.¹⁶⁵


В этой быстроизменяющейся среде важно отслеживать, какие технологии в настоящий момент разрабатываются и развертываются в России и Китае, чтобы спрогнозировать, что в скором времени появится в других странах мира. Разумеется, такие страны, как Иран, Таиланд или Венесуэла разрабатывают собственные методы и технологии. Однако широкое распространение средств контроля информации китайского и российского производства в мире может служить важной точкой отсчета для распознавания будущих тенденций до их широкого распространения в мире.



Что же делать демократическим государствам в свете подобных тенденций? К сожалению, простого ответа не существует, отчасти из-за того, что трудно предотвратить распространение технологий и методик двойного назначения (не считая того факта, что демократические государства и сами охотно приобретают оборудование для контроля информации). А когда предлагаемые стажировки рекламируются как безобидные учебные программы, а не обучение стратегическим методам распространения информации, их непросто критиковать.

Тем не менее, демократические государства все же могут принять меры. На собственной территории у них нет необходимости внедрять все средства слежения и наблюдения. В штате Массачусетс рассматривается законопроект об ограничении использования технологий распознавания лиц.¹⁶⁶ Городские власти Сан-Франциско уже приняли подобные положения.¹⁶⁷ Когда речь идет о собственных компаниях, вовлеченных в проекты по созданию технологий для цензуры и слежки, демократические государства должны убедиться, что эти проекты не влекут нарушений прав человека, а компании не являются соучастниками подобных нарушений.¹⁶⁸

Демократические государства также должны работать над тем, чтобы индивидуальные устройства и каналы связи, которыми пользуются граждане, были лучше защищены от действия оборудования для фильтрации и слежки. На данный момент ситуация прямо противоположная. Недавно, в Австралии был принят закон, расширяющий наблюдение за трафиком и ограничивающий возможность сквозного шифрования сообщений — шаг, более характерный для авторитарного государства.¹⁶⁹ Канада, Новая Зеландия, Великобритания и США намереваются создать подобные точки доступа для властей и у себя.¹⁷⁰ Эти действия не являются необходимостью для обеспечения безопасности. Согласно имеющимся исследованиям, даже без доступа к текстам сообщений у государственных органов имеется в распоряжении множество средств борьбы с преступностью.¹⁷¹ Существование сквозного шифрования еще не означает, что



государство «ослепло». В частности, для расследования преступлений могут быть использованы метаданные, которые зачастую куда более полезны чем собственно содержимое сообщений.


Наконец, очевидно, что в демократических государствах использование средств слежки и наблюдения должно подпадать под прозрачные правила с возможностью общественного контроля. Например, необходима система сдержек и противовесов для ограничения доступа к данным систем наблюдения со стороны разведывательных служб там, где они предназначены только для использования местной полицией.¹⁷²

Хотя ни одно из этих предложений не может само по себе воспрепятствовать распространению технологий наблюдения и слежки в мире, в комбинации они теоретически могут предотвратить некоторые злоупотребления в будущем.

В целом ситуация со свободой слова и правами человека в мире ухудшается. На сегодняшний день, более ста государств приобрели или копировали средства контроля информации из России и Китая, а также получили возможность подготовить в этих странах своих специалистов по использованию технологий. В такой ситуации демократические государства должны воспрепятствовать распространению авторитарных подходов к использованию технологий и показать миру, что бороться с преступностью и обеспечивать национальную безопасность возможно и без урона кибербезопасности и частной жизни граждан в интернете. Это несомненно непростая задача, но к этому следует стремиться. Ведь если демократические государства ничего не предпримут, кто сделает это за них?

БЛАГОДАРНОСТИ

Я очень обязан Лукасу Калло (Lucas Kello) и Джоссу Райту (Joss Wright) за их продуманные советы и рекомендации, сделанные на различных этапах проекта.



Мне также были очень полезны комментарии, полученные от Ирен Поэтранто (Irene Poetranto), Габриэль Лим (Gabrielle Lim), Макса Кухель-Бугарича (Max Kuhelj-Bugaric), Джонаса Кайзера (Jonas Kaiser) и Дина Джексона (Dean Jackson). Очень благодарен Центру Беркмана Клейна по исследованиям интернета и общества в Гарвардском университете за возможность воспользоваться полным жизни местом для своих размышлений, Фонду открытых технологий и Британскому совету по инженерным и физическим научным исследованиям за любезно оказанное ими содействие моей работе.

ПРИЛОЖЕНИЕ 1: ТАБЛИЦА РАСПРОСТРАНЕНИЯ

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
Страны		Китай	Россия	Китай	Россия	Китай	Россия
Алжир К(1) Р(1)	A ¹⁷³	X ¹⁷⁴	X ¹⁷⁵				
Ангола К(2)	A	X ¹⁷⁶				X ¹⁷⁷	
Антигуа и Барбуда К(1)	/					X ¹⁷⁸	
Аргентина К(2)	Д	X ¹⁷⁹				X ¹⁸⁰	
Армения К(1)	Г					X ¹⁸¹	
Австралия К(1)	Д					X ¹⁸²	
Азербайджан К(1) Р(2)	A	X ¹⁸³	X ¹⁸⁴		X ¹⁸⁵		
Багамы К(1)	/					X ¹⁸⁶	
Бангладеш К(1)	Г					X ¹⁸⁷	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Страны							
Барбадос К(1)	/					X ¹⁸⁸	
Беларусь К(2) Р(2)	А	X ¹⁸⁹	X ¹⁹⁰		X ¹⁹¹	X ¹⁹²	
Боливия К(1)	Г	X ¹⁹³					
Ботсвана К(1)	Д					X ¹⁹⁴	
Бразилия К(1)	Д	X ¹⁹⁵					
Камбоджа К(2)	А	X ¹⁹⁶				X ¹⁹⁷	
Камерун К(2)	А	X ¹⁹⁸				X ¹⁹⁹	
Чад К(1)	А					X ²⁰⁰	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Страны Центральн оафриканс кая республик а К(1)	А					Х ²⁰¹	
Чили К(1)	Д	Х ²⁰²					
Китай Р(1)	А	Н/Д		Н/Д	Х ²⁰³	Н/Д	
Колумбия К(2) Р(1)	Д	Х ²⁰⁴	Х ²⁰⁵			Х ²⁰⁶	
Коморские острова Р(1)	А		Х ²⁰⁷				
Конго К(1)	А					Х ²⁰⁸	

Страны	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Кот-д'Ивуар К(2)	Г	Х ²⁰⁹				Х ²¹⁰	
Куба К(1) Р(1)	А	Х ²¹¹	Х ²¹²				
Доминика К(1)	/					Х ²¹³	
Эквадор К(2) Р(1)	Д	Х ²¹⁴	Х ²¹⁵			Х ²¹⁶	
Египет К(3)	А	Х ²¹⁷		Х ²¹⁸		Х ²¹⁹	
Эритрея К(1)	А					Х ²²⁰	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
Страны		Китай	Россия	Китай	Россия	Китай	Россия
Эфиопия К(2)	А	χ^{221}				χ^{222}	
Франция К(1)	Д	χ^{223}					
Гамбия К(1)	Г					χ^{224}	
Германия К(1)	Д	χ^{225}					
Гана К(2)	Д	χ^{226}				χ^{227}	
Гренада К(1)	/					χ^{228}	
Гвинея К(1)	А					χ^{229}	
Гайана К(1)	Д					χ^{230}	
Венгрия К(1)	Д	χ^{231}					

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Страны							
Индия К(1) Р(1)	Д		Х ²³²			Х ²³³	
Индонезия К(2)	Д	Х ²³⁴				Х ²³⁵	
Иран К(3)	А	Х ²³⁶		Х ²³⁷		Х ²³⁸	
Ирак К(1)	Г	Х ²³⁹					
Ирландия К(1)	Д	Х ²⁴⁰					
Иордания К(1)	А	Х ²⁴¹					
Италия К(1)	Д	Х ²⁴²					
Ямайка К(1)	Д					Х ²⁴³	
Казахстан К(2) Р(2)	А	Х ²⁴⁴	Х ²⁴⁵		Х ²⁴⁶	Х ²⁴⁷	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
Страны		Китай	Россия	Китай	Россия	Китай	Россия
Кения К(2)	Г	χ^{248}				χ^{249}	
Кыргызстан К(2) Р(2)	Г	χ^{250}	χ^{251}		χ^{252}	χ^{253}	
Лаос К(2)	А	χ^{254}				χ^{255}	
Лесото К(1)	Д					χ^{256}	
Либерия К(1)	Г					χ^{257}	
Ливия К(1)	А	χ^{258}					
Литва Р(1)	Д		χ^{259}				
Малави К(1)	Г					χ^{260}	
Малайзия К(3)	Д	χ^{261}		χ^{262}		χ^{263}	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Страны							
Мальдивы P(1)	/		Х ²⁶⁴				
Мали K(1)	Г					Х ²⁶⁵	
Мавритан ия K(1)	Д	Х ²⁶⁶					
Мексика K(1) P(1)	Д	Х ²⁶⁷	Х ²⁶⁸				
Молдова K(1) P(1)	Г	Х ²⁶⁹			Х ²⁷⁰		
Монголия K(2)	Д	Х ²⁷¹				Х ²⁷²	
Марокко K(2)	Г	Х ²⁷³				Х ²⁷⁴	
Мозамбик K(2)	А	Х ²⁷⁵				Х ²⁷⁶	

Страны	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Мьянма К(2)	А	Х ²⁷⁷				Х ²⁷⁸	
Непал Р(1)	Г		Х ²⁷⁹				
Нидерланды К(1)	Д	Х ²⁸⁰					
Никарагуа Р(1)	А		Х ²⁸¹				
Нигер Р(2)	А	Х ²⁸²				Х ²⁸³	
Нигерия К(2)	Г	Х ²⁸⁴				Х ²⁸⁵	
Норвегия К(1)	Д	Х ²⁸⁶					
Пакистан К(2)	Г	Х ²⁸⁷				Х ²⁸⁸	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Страны							
Палестина P(1)	Г		Х ²⁸⁹				
Перу K(1)	Д					Х ²⁹⁰	
Филиппины K(2)	Д	Х ²⁹¹				Х ²⁹²	
Польша K(1)	Д	Х ²⁹³					
Румыния K(1)	Д	Х ²⁹⁴					
Россия K(3)	А	Х ²⁹⁵	Н/Д	Х ²⁹⁶	Н/Д	Х ²⁹⁷	Н/Д
Руанда K(1)	А					Х ²⁹⁸	
Саудовская Аравия K(2) P(1)	А	Х ²⁹⁹	Х ³⁰⁰			Х ³⁰¹	
Сенегал K(1)	Д	Х ³⁰²					

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
Страны		Китай	Россия	Китай	Россия	Китай	Россия
Сербия К(1)	Д	Х ³⁰³					
Сейшелы К(1)	/					Х ³⁰⁴	
Сьерра-Леоне К(2)	Г	Х ³⁰⁵				Х ³⁰⁶	
Сингапур К(2) Р(1)	Д	Х ³⁰⁷	Х ³⁰⁸			Х ³⁰⁹	
ЮАР К(2)	Д	Х ³¹⁰				Х ³¹¹	
Южная Корея К(2)	Д	Х ³¹²				Х ³¹³	
Южный Судан К(1)	/					Х ³¹⁴	
Испания К(1)	Д	Х ³¹⁵					
Шри Ланка К(2)	Д	Х ³¹⁶				Х ³¹⁷	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Страны Судан К(2)	А	Х ³¹⁸				Х ³¹⁹	
Суринам С(1)	Д					Х ³²⁰	
Таджикистан К(2) Р(1)	А	Х ³²¹	Х ³²²			Х ³²³	
Танзания К(3)	Г	Х ³²⁴		Х ³²⁵		Х ³²⁶	
Таиланд К(3) Р(1)	Г	Х ³²⁷	Х ³²⁸	Х ³²⁹		Х ³³⁰	
Тринидад и Тобаго К(2)	Д	Х ³³¹				Х ³³²	
Турция К(2), Р(1)	Г	Х ³³³	Х ³³⁴			Х ³³⁵	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Страны Туркменистан К(1), Р(1)	А		Х ³³⁶			Х ³³⁷	
Уганда К(3)	Г	Х ³³⁸		Х ³³⁹		Х ³⁴⁰	
Украина К(1), Р(2)	Г	Х ³⁴¹	Х ³⁴²		Х ³⁴³		
Объединенные Арабские Эмираты К(1)	А	Х ³⁴⁴					
Великобритания К(2)	Д	Х ³⁴⁵				Х ³⁴⁶	
Соединенные Штаты Америки К(2), Р(1)	Д	Х ³⁴⁷	Х ³⁴⁸			Х ³⁴⁹	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
		Китай	Россия	Китай	Россия	Китай	Россия
Страны Уругвай К(1)	Д	Х ³⁵⁰					
Узбекистан К(2) Р(2)	А	Х ³⁵¹	Х ³⁵²		Х ³⁵³	Х ³⁵⁴	
Венесуэла К(3)	А	Х ³⁵⁵		Х ³⁵⁶		Х ³⁵⁷	
Вьетнам К(2)	А			Х ³⁵⁸		Х ³⁵⁹	
Йемен Р(1)	А		Х ³⁶⁰				
Замбия К(3)	Г	Х ³⁶¹		Х ³⁶²		Х ³⁶³	

	Тип режима	Технологии фильтрации и слежки		Имитация		Обучение	
Страны		Китай	Россия	Китай	Россия	Китай	Россия
Зимбабве К(3)	А	χ^{364}		χ^{365}		χ^{366}	
Итого (из 110)		73	26	11	8	75	0
Проникновение российского подхода		Российская модель контроля за информацией проникает в 28 стран					
Проникновение китайского подхода		Китайская модель контроля за информацией проникает в 102 странах					
Совместное проникновение		Российский и китайский подходы к контролю за информацией проникают в 110 стран (включая проникновение российской модели в Китай и наоборот). Контроль информации экспортируется в 41 демократическую страну, в 24 страны с гибридным режимом и в 37 авторитарных Economist Intelligence Unit не предоставляет тип режима для 8 исследованных стран - Антигуа и Барбуда, Багам, Барбадоса, Доминики, Гренады, Мальдив, Сейшел и Южного Судана.					



ПРИЛОЖЕНИЕ 2: СПИСОК КИТАЙСКИХ КОМПАНИЙ

Компания	Тип технологии / проникновения	Местонахождение	Охват
Alcatel-Lucent Shanghai Bell Co.	Оборудование совместимое с СОРМ	Шанхай	Казахстан
Alibaba Group	Управление трафиком на базе ИИ	Ханчжоу	Малайзия
Baifendian / Percent Corporation	Управления большими базами данных с помощью ИИ	Пекин	Ангола
CEIEC (Государственная корпорация по импорту-экспорту электроники)	Безопасные города	Пекин	Эквадор, Тринидад и Тобаго, Уганда, Венесуэла
CloudWalk Technology	Камеры с системой распознавания лиц	Пекин	Зимбабве
Dahua Technology Co.	Камеры с распознаванием лиц	Ханчжоу	Танзания
Hikvision	Камеры с распознаванием лиц	Ханчжоу	Аргентина, Бразилия, Великобритания, Египет, Зимбабве, Ирландия, Иордания, Мьянма, Таиланд, Украина ЮАР, Южная Корея,
Huaneng Industry	Поддержка тренингов для медиа	Пекин	Бангладеш, Малайзия

Компания	Тип технологии / проникновения	Местонахождение	Охват
Huawei	Технологии цензурирования, камеры с распознаванием лиц, безопасный город, содействия властям в доступе к зашифрованным коммуникациям	Шэньжень	Алжир, Азербайджан, Беларусь, Боливия, Венгрия, Венесуэла, Германия, Египет, Замбия, Индонезия, Иран, Ирак, Испания, Италия, Кения, Камерун, Колумбия, Кот-д'Ивуар, Куба, Лаос, Мексика, Молдова, Марокко, Мозамбик, Нигер, Нигерия, Нидерланды, Норвегия, ОАЭ, Пакистан, Польша, Россия, Саудовская Аравия, Сербия, Сингапур, США, Таджикистан, Таиланд, Танзания, Тринидад и Тобаго, Турция, Уганда, Украина, Филиппины, Франция, Чили, Эквадор

Компания	Тип технологии / проникновения	Местонахождение	Охват
Meiya Pico	Цифровая криминалистика и тренинги по кибербезопасности	Сямынь	Аргентина, Армения, Бангладеш, Беларусь, Великобритания, Вьетнам, Камбоджа, Колумбия, Эквадор, Египет, Индия, Индонезия, Кыргызстан, Казахстан, Лаос, Малайзия, Моголия, Марокко, Мьянма, Пакистан, Филиппины, Россия, Саудовская Аравия, Таиланд, Таджикистан, Турция, США,
SenseTime	Динамические системы распознавания лиц	Пекин	Монголия
Yitu	Камеры с распознаванием лиц	Шанхай	Малайзия
ZTE	Технологии цензуры, безопасный город	Шэньчжэнь	Беларусь, Венесуэла, Замбия, Ливия, Румыния, Сенегал, Сьерра-Леоне, Судан, Уругвай, Шри Ланка, Эфиопия

ПРИЛОЖЕНИЕ 3: СПИСОК ОРГАНИЗАЦИЙ, СВЯЗАННЫХ С КИТАЕМ

Организация	Роль	Местонахождения	Охват
Институт Австралийско-Китайский отношений	Организация образовательных стажировок для журналистов в Китае	Сидней, Австралия	Австралия
Посольство Китая на Филиппинах	Медиа-тренинги для журналистов и официальных лиц	Пекин	Филиппины
Международная китайская издательская группа	Медиа-тренинги для журналистов и официальных лиц	Пекин	Филиппины

Организация	Роль	Местонахождения	Охват
Китайская ассоциация общественной дипломатии	Координация медиа тренингов	Пекин	Ангола, Антигуа и Барбуда, Багамы, Барбадос, Ботсвана, Гамбия, Гана, Гвинея, Гайана, Гренада, Доминика, Египет, Камурун, Кения, Конго, Кот-д'Ивуар, Лесото, Либерия, Малави, Мали, Мозамбик, Нигер, Нигерия, Пакистан, Руанда, Сейшеллы, Сьера-Леоне, Уганда, Чад, Центрально-африканская республика, Эритрея, ЮАР, Южный Судан
Фонд обмена Китай - США	Организация поездок журналистов в Китай	Гонконг	США
Китайский университет коммуникаций	Проведение медиатренингов	Пекин	Бангладеш, Малайзия
Информационный совет / Государственный совет информационного офиса	Распространение методов контроля информации среди официальных лиц и журналистов	Пекин	Иран, Филиппины

Организация	Роль	Местонахождения	Охват
Отдел кадров коммунистической партии региона Гуанси	Управляет академией лидерства Baize	регион Гуанси	Вьетнам, Лаос, Мьянма
Министерство торговли	Медиа-тренинги для журналистов и официальных лиц	Пекин	Филиппины
Министерство образования	Поддерживает медиа-тренинги	Пекин	Бангладеш, Малайзия
Министерство иностранных дел	Поддерживает медиа-тренинги	Пекин	Бангладеш, Малайзия
Министерство общественной безопасности	Сотрудничает по вопросам оборудования для слежки с камбоджийскими правоохранительными органами	Пекин	Камбоджа
Разведывательное управление народно-освободительной армии	Обучение официальных лиц контролю над информацией	Пекин	Шри Ланка
Университет Цинхуа	Программа глобальной бизнес-журналистики	Пекин	Южная Корея

ПРИЛОЖЕНИЕ 4: СПИСОК РОССИЙСКИХ КОМПАНИЙ

Компания	Тип технологии / проникновения	Местонахождение	Охват
Аналитические Бизнес-решения	Инструменты для анализа открытых данных в форумах и социальных медиа	Москва	Беларусь, Казахстан
iТесо	Инструменты для анализа открытых данных в форумах и социальных медиа	Москва	Казахстан
МФИ Софт	Оборудование СОРМ	Нижний Новгород и Москва	Казахстан, Таджикистан, Узбекистан
Оникс-Лайн	Оборудование СОРМ	Москва	Кыргызстан
Oxygen Software	Криминалистика мобильной связи	Москва	Казахстан, Узбекистан

Компания	Тип технологии / проникновения	Местонахождение	Охват
НТЦ Протей	Оборудование СОРМ	Санкт-Петербург	Коморы, Куба, Казахстан, Палестина, Таджикистан, Узбекистан
Сигнатек	Оборудование СОРМ	Novosibirsk	Кыргызстан
Центр речевых технологий / SpeechPro	аудио криминалистика / распознавание лиц	Санкт-Петербург	Алжир, Индия, Йемен, Колумбия, Казахстан, Мальдивы, Мексика, Непал, Саудовская Аравия, Сингапур, США, Туркменистан, Турция, Узбекистан, Эквадор

Компания	Тип технологии / проникновения	Местонахождение	Охват
VAS Experts	Оборудование СОПМ	Санкт-Петербург	Азербайджан, Казахстан, Литва, Никарагуа, Узбекистан

¹ Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, August 15, 2019, sec. Tech, <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017>; Sheridan Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain," January 10, 2019, <https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain>; Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, <https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html>; Andrei Soldatov and Irina Borogan, "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact," *The Guardian*, November 29, 2016, sec. World news, <https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact>.

² Stabroek News, "China Launches Press Programme to Improve Ties with Caribbean," *Stabroek News*, April 8, 2018, <https://www.stabroeknews.com/2018/news/guyana/04/08/china-launches-press-programme-to-improve-ties-with-caribbean/>; Irina Borogan and Andrei Soldatov, "Just Business: How Russian Technology Provides the Eyes and Ears for the World's Big Brothers," *OpenDemocracy*, January 25, 2012, <http://www.opendemocracy.net/od-russia/andrei-soldatov-irina-borogan/just-business-how-russian-technology-provides-eyes-and-ears->.

³ Jianfeng Zhang, "China-Caribbean Press Center Launched," April 19, 2018, <http://english.cctv.com/2018/04/19/ARTIBzkdnQ3Ld2GWuohcBiSd180419.shtml>; Fredrick P. W. Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China," *People's Daily Online*, December 2, 2016, 28, <http://en.people.cn/n3/2016/1202/c90000-9150101.html>; Juan Pablo Cardenal, "China in Latin America: Understanding the Inventory of Influence," in *Sharp Power: Rising Authoritarian Influence* (National Endowment for Democracy, 2017), <https://www.ned.org/wp-content/uploads/2017/12/Chapter1-Sharp-Power-Rising-Authoritarian->

Influence-China-Latin-America.pdf; Hikvision, "Hikvision's Products Deployed in Military Command of the East in Brazil," April 21, 2010, <https://www.hikvision.com/en/Press/Success-Stories/Government/305528967821644>; Hikvision, "Total Control for Jordan's House of Parliament," March 31, 2016, <https://www.hikvision.com/en/Press/Success-Stories/Government/305528977464530>.

⁴ VAS Experts, "About Us," *VAS Experts*, 2019, <https://vasexpertsdpi.com/about-us/>; Borogan and Soldatov, "Just Business"; Protei, "Past Events," accessed January 18, 2019, <http://www.protei.com/events/past/>; Protei, "News and Events - Protei MENA," accessed January 18, 2019, <http://protei.me/News-and-Events>.

⁵ Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance* 18 (2012). p. 339.

⁶ Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton N.J.: Princeton University Press, 2018).

⁷ Bruce Schneier, "Click Here to Kill Everyone," 2017, <https://nymag.com/intelligencer/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html>.

⁸ Erika Kinetz, "In China, Your Car Could Be Talking to the Government," *AP NEWS*, November 29, 2018, <https://apnews.com/c6e610eb8f4645b4806bc16479b64809>.

⁹ Frederick Schauer, "Fear, Risk and the First Amendment: Unraveling the Chilling Effect" (College of William & Mary Law School, 1978), <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=2010&context=facpubs>; Marilyn Clark and Anna Grech, "Journalists Under Pressure - Unwarranted Interference, Fear and Self-Censorship in Europe" (Council of Europe, 2017), <https://rm.coe.int/168070ad5d>; Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review* 154, no. 3 (January 1, 2006): 477, doi:10.2307/40041279.

¹⁰ Andrew F. Hayes, Carroll J. Glynn, and James Shanahan, "Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research," *International Journal of Public Opinion Research* 17, no. 3 (2005): 298–323, doi:10.1093/ijpor/edh073.

¹¹ Там же.

¹² Там же.

¹³ Тор является программным обеспечением, позволяющим анонимное общение и таким образом позволяющее пользователям ускользнуть от слежки.

¹⁴ Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, February 7, 2019), <https://papers.ssrn.com/abstract=3330413>.

¹⁵ Jonathan Auerbach and Russ Castronovo, "Introduction: Thirteen Propositions About Propaganda," in *The Oxford Handbook of Propaganda Studies*, 2013, <https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199764419.001.0001/oxfordhb-9780199764419-e-023>; Gabrielle Lim, "Disinformation Annotated Bibliography" (Citizen Lab, May 2019), <https://citizenlab.ca/wp-content/uploads/2019/05/Disinformation-Bibliography.pdf>.

¹⁶ Adam B. Ellick and Adam Westbrook, "Operation Infektion: A Three-Part Video Series on Russian Disinformation," *The New York Times*, November 1, 2018, <https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html>.

¹⁷ Jesper Schlæger and Min Jiang, "Official Microblogging and Social Management by Local Governments in China," 2014,

<https://journals.sagepub.com/doi/full/10.1177/0920203X14533901>.

¹⁸ Sina Weibo, "微博-随时随地发现新鲜事," n.d., <https://www.weibo.com/login.php>.

¹⁹ Max Seddon and Henry Foy, "Russian Technology: Can the Kremlin Control the Internet?," *Financial Times*, June 5, 2019, <https://www.ft.com/content/93be9242-85e0-11e9-a028-86cea8523dc2>.

²⁰ Cyberspace Administration of China, "Internet Forum Community Service Management Regulations," August 25, 2017, http://www.cac.gov.cn/2017-08/25/c_1121541921.htm; Benjamin Haas, "Man in China Sentenced to Five Years' Jail for Running VPN," *The Guardian*, December 22, 2017, sec. World news, <http://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn>.

²¹ Jakub Dalek, *Russian Blacklist*, Python, (2014; repr., 2018), <https://github.com/jakubd/russian-blacklist>.

²² В данном докладе анализирует российский и китайский подход к контролю за информацией, но также могут существовать страны, использующие схожие подходы для контроля за информацией без прямого взаимодействия с российскими/китайскими технологиями, методами или обучением. Это случаи развития независимой модели контроля за информацией. Например, небольшое островное государство в Тихом океане могло создать комплекс правовых и внеправовых решений для запуска самоцензуры среди населения, в то же время наводнив социальные медиа провластными сообщениями. Это не значит, что страна внедряет контроль за информацией по российской модели, а что она независимо разработала такой метод управления информацией. Другие страны в свою очередь нашли другие подходы к цензурированию онлайн-пространство. Хотя Индия воспринимает китайский и российский подход к контролю за информацией, она активно использует отключение сети для контроля диссидентов, решение, не используемое Китаем и Россией в таких масштабах.

²³ Jaclyn Kerr, "The Russian Model of Internet Control and Its Significance," LLNL-TR-764577 (Lawrence Livermore National Laboratory, December 21, 2018).

²⁴ Privacy International, "Lawful Interception: The Russian Approach," March 4, 2013, <https://privacyinternational.org/blog/1296/lawful-interception-russian-approach>.

²⁵ Russian Federation, "Information Security Doctrine of the Russian Federation" (2000), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf.

²⁶ Kerr, "The Russian Model of Internet Control and Its Significance."

²⁷ Masha Gessen, "Reporting Within the Lines in Putin's Russia," *The New York Times*, July 15, 2016, sec. Opinion, <https://www.nytimes.com/2016/07/15/opinion/reporting-within-the-lines-in-putins-russia.html>.

²⁸ Radio Free Europe / Radio Liberty, "U.S. Lawmakers Overwhelmingly Condemn Kremlin For Nemtsov Killing," *RadioFreeEurope/RadioLiberty*, March 13, 2019, <https://www.rferl.org/a/russia-nemtsov-putin-killing/29818275.html>; Marc Bennetts, "Russian Opposition Leader Alexei Navalny Jailed for 30 Days," *The Guardian*, August 27, 2018, sec. World news, <https://www.theguardian.com/world/2018/aug/27/russian-opposition-leader-alexei-navalny-jailed-for-30-days>; Danny Hakim, "Once Celebrated in Russia, the Programmer Pavel Durov

Chooses Exile," *The New York Times*, December 21, 2017, sec. Technology, <https://www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html>.

²⁹ Erik C. Nisbet, Olga Kamenchuk, and Aysenur Dal, "A Psychological Firewall? Risk Perceptions and Public Support for Online Censorship in Russia," *Social Science Quarterly* 98, no. 3 (2017): 958–75.

³⁰ John D. Gallacher and Rolf E. Fredheim, "Division Abroad, Cohesion at Home: How the Russian Troll Factory Works to Divide Societies Overseas but Spread Pro-Regime Messages at Home," in *Responding to Cognitive Security Challenges* (Latvia: NATO STRATCOM Centre of Excellence, 2019).

³¹ Там же.; BBC, "Russia Profile - Media," April 25, 2017, sec. Europe, <https://www.bbc.com/news/world-europe-17840134>.

³² Miriam Elder, "Hacked Emails Allege Russian Youth Group Nashi Paying Bloggers," *The Guardian*, February 7, 2012, sec. World news, <https://www.theguardian.com/world/2012/feb/07/hacked-emails-nashi-putin-bloggers>; Shaun Walker, "The Russian Troll Factory at the Heart of the Meddling Allegations," *The Guardian*, April 2, 2015, sec. World news, <https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house>.

³³ Walker, "The Russian Troll Factory at the Heart of the Meddling Allegations."

³⁴ Federal Antimonopoly Service of the Russian Federation, "Yandex vs. Google," June 27, 2016, <http://en.fas.gov.ru/documents/documentdetails.html?id=14677>; Brendan McGonigle, "Yandex Catches Google on Android in Russia," *Russian Search Marketing*, August 28, 2018, <https://russiansearchmarketing.com/yandex-catches-google-on-android-in-russia/>; Statcounter, "Social Media Stats Russian Federation," *StatCounter Global Stats*, accessed April 30, 2019, <http://gs.statcounter.com/social-media-stats/all/russian-federation>.

³⁵ Dalek, *Gets a Simple Dump of the Russian Federal Black List of Blocked Sites from the Excellent Antizapret.Info in a Few Formats*; Seddon and Foy, "Russian Technology."

³⁶ Алексей Навальный, "Алексей Навальный," *YouTube*, accessed March 19, 2019, <https://www.youtube.com/channel/UCsAw3WynQJmM7tMy093y37A>.

³⁷ Matt Burgess, "This Is Why Russia's Attempts to Block Telegram Have Failed," *Wired UK*, April 28, 2018, <https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google>.

³⁸ Ryan Browne, "Russia Follows China in VPN Clampdown, Raising Censorship Concerns," *CNBC*, July 31, 2017, <https://www.cnn.com/2017/07/31/russia-follows-china-in-vpn-clampdown-raising-censorship-concerns.html>; Vasilis Ververis et al., "Shedding Light on Mobile App Store Censorship," in *UMAP'19 Adjunct Adjunct Publication of the 27th Conference on Modeling, Adaptation and Personalization* (Larnaca, Cyprus and New York NY: ACM, 2019), <https://dl.acm.org/citation.cfm?id=3324965>.

³⁹ Joseph Cox and Emanuel Maiberg, "Chinese Government Forces Residents To Install Surveillance App With Awful Security," *Vice*, April 9, 2018, https://www.vice.com/en_us/article/ne94dg/jingwang-app-no-encryption-china-force-install-urumqi-xinjiang; Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," April 14, 2019, <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>.

-
- ⁴⁰ Yujie Xue, "Camera Above the Classroom," *Sixth Tone*, March 26, 2019, <https://www.sixthtone.com/news/1003759/camera-above-the-classroom>; Karen Hao, "China's Government Has Given Location-Tracking Watches to 17,000 Children," *MIT Technology Review*, July 18, 2019, <https://www.technologyreview.com/f/613978/china-gps-beidou-gives-location-tracking-watches-to-17-000-children-privacy/>.
- ⁴¹ Jonathon W. Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal* 31, no. 1 (2016): 118–82.
- ⁴² Josh Chin, "New Target for China's Censors: Content Driven by Artificial Intelligence," *Wall Street Journal*, April 11, 2018, sec. Tech, <https://www.wsj.com/articles/new-target-for-chinas-censors-content-driven-by-artificial-intelligence-1523446234>.
- ⁴³ Tao Zhu et al., "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions" (USENIX Security Symposium, Washington, D.C., 2013), <https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/zhu>.
- ⁴⁴ Ray Bradbury, *Fahrenheit 451*, Reissue edition (New York; Toronto: Simon & Schuster, 2012).
- ⁴⁵ Ververis et al., "Shedding Light on Mobile App Store Censorship."
- ⁴⁶ Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 03 (August 2017): 484–501, doi:10.1017/S0003055417000144.
- ⁴⁷ Rongbin Han, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army,'" *Journal of Current Chinese Affairs* 2 (2015): 105–34.
- ⁴⁸ Lei Zhang, "Invisible Footprints of Online Commentators," *Global Times*, February 5, 2010, <http://www.globaltimes.cn/special/2010-02/503820.html>.
- ⁴⁹ King, Pan, and Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument."
- ⁵⁰ Там же.; Yuan Yang, "China's Communist Party Raises Army of Nationalist Trolls," *Financial Times*, December 30, 2017, <https://www.ft.com/content/9ef9f592-e2bd-11e7-97e2-916d4fbac0da>.
- ⁵¹ Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*, p. 94.
- ⁵² Там же, pp. 13–14.
- ⁵³ Haas, "Man in China Sentenced to Five Years' Jail for Running VPN"; Cyberspace Administration of China, "Internet Forum Community Service Management Regulations."
- ⁵⁴ Mindy K. Longanecker, "No Room for Dissent: China's Laws Against Disturbing Social Order Undermine Its Commitments to Free Speech and Hamper the Rule of Law," *Pacific Rim Law & Policy Journal* 18, no. 2 (April 2009): 373–403.
- ⁵⁵ Достоверных подтверждений российских образовательных программ зарубежом найдено не было - соответственно, только два индикатора применяются для России.
- ⁵⁶ Hikvision, "Hikvision Gives Japan a Culturally and Technically Relevant Solution," December 1, 2011, <https://www.hikvision.com/en/Press/Success-Stories/Education/305528882360250>.
- ⁵⁷ For more information on surveillance middleboxes See Jakub Dalek et al., "Planet Netsweeper: Executive Summary," *The Citizen Lab*, April 25, 2018, <https://citizenlab.ca/2018/04/planet-netsweeper/>.
- ⁵⁸ Maria Xynou, Arturo Filastò, and Simone Basso, "Measuring Internet Censorship in Cuba's ParkNets," *OONI - Open Observatory of Network Interference*, August 28, 2017, <https://ooni.torproject.org/post/cuba-internet-censorship-2017/>; Huawei, "HUAWEI ESight

Network Full Product Datasheet," *Huawei Enterprise*, 2017,
<https://e.huawei.com/uk/material/esight/e60e006763444062a048bc83f1965ebf>.

⁵⁹ "Colombia," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Colombia_AS262928; Xynou, Filastò, and Basso, "Measuring Internet Censorship in Cuba's ParkNets"; "Italy," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Italy_AS203469; "Mexico," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Mexico_AS22908; Censys, "V2R2C00-IAE/1.0," Censys, accessed July 9, 2019, http://tiny.cc/Nigeria_AS; "Pakistan," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Pakistan_AS45773; "Spain," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Spain_AS12430; "Turkey," OONI Explorer, accessed June 17, 2019, http://tiny.cc/Turkey_AS201411.

⁶⁰ Borogan and Soldatov, "Just Business."

⁶¹ Asterius Banzi, "Tanzania: Govt Seeks Chinese Help in Social Media," *The East African (Nairobi)*, August 1, 2017, <https://allafrica.com/stories/201708020658.html>; Lincoln Towindo, "Government to Regulate Social Media," April 10, 2016, <http://www.sundaymail.co.zw/social-media-regulation-is-nigh/>.

⁶² Louisa Lim and Julia Bergin, "Inside China's Audacious Plan for Global Media Dominance," *The Guardian*, December 7, 2018, <https://www.theguardian.com/news/2018/dec/07/china-plan-for-global-media-dominance-propaganda-xi-jinping>.

⁶³ Cardenal, "China in Latin America: Understanding the Inventory of Influence."

⁶⁴ Huifeng He, "In a Remote Corner of China, Beijing Is Trying to Export Its Model by Training Foreign Officials the Chinese Way," *South China Morning Post*, July 14, 2018, <https://www.scmp.com/news/china/economy/article/2155203/remote-corner-china-beijing-trying-export-its-model-training>.

⁶⁵ The Economist Intelligence Unit also distinguished between full democracy and flawed democracy, a distinction which is not made explicitly in this paper. The Economist, "The Retreat of Global Democracy Stopped in 2018," *The Economist*, January 8, 2019, <https://www.economist.com/graphic-detail/2019/01/08/the-retreat-of-global-democracy-stopped-in-2018>.

⁶⁶ Kurt Weyland, "Crafting Counterrevolution: How Reactionaries Learned to Combat Change in 1848" 110, no. 2 (2016): 215–31, doi:10.1017/S0003055416000174.

⁶⁷ Там же.

⁶⁸ У оставшихся 7% стран Индекс демократии Economist не определил тип режима (см. Список стран Приложении 1).

⁶⁹ Hikvision, "Hikvision and Argentina: Working Together for a Safer Tomorrow," August 4, 2011, <https://www.hikvision.com/en/Press/Success-Stories/City-Surveillance/305528874961488>; Huawei, "Huawei Smart City Solution," 2013, https://www.iotone.com/files/pdf/vendor/Huawei_Smart_City_Solution_2013.pdf; Xinhua, "华为助力法国打造'平安城市'-新华网," February 10, 2017, http://www.xinhuanet.com/world/2017-02/10/c_1120445581.htm; Huawei, "Gelsenkirchen: A Small, Smart City with Big Plans," *Huawei Enterprise*, 2017, <https://e.huawei.com/us/case-studies/global/2017/201709071445>; Huawei Enterprise, "Smart City: Sardinia Italy," *Huawei Enterprise*, accessed January 20, 2019, <https://e.huawei.com/en/videos/global/2018/201804101040>; Huawei Enterprise, "Spain

Enhances Smart City with ELTE Solution," *Huawei Enterprise*, 2018, <https://e.huawei.com/us/case-studies/global/2018/201807041019>.

⁷⁰ Glasius defines "authoritarian practices as patterns of action that sabotage accountability to people over whom a political actor exerts control or their representatives, by means of secrecy, disinformation and disabling voice. These are distinct from illiberal practices, which refer to patterned and organized infringements of individual autonomy and dignity." Marlies Glasius, "What Authoritarianism Is ... and Is Not: A Practice Perspective," *International Affairs* 94, no. 3 (2018): 515–33, doi:10.1093/ia/iyy060.

⁷¹ Там же.

⁷² Joseph Menn, "Microsoft Turned down Facial-Recognition Sales on Human Rights Concerns," April 16, 2019, <https://www.reuters.com/article/us-microsoft-ai/microsoft-turned-down-facial-recognition-sales-on-human-rights-concerns-idUSKCN1RS2FV>.

⁷³ Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance"; Meiya Pico, "Training," 2019, <https://meiyapico.com/training/index.html>.

⁷⁴ Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance"; Meiya Pico, "Training."

⁷⁵ Steven Levitsky and Lucan Way, "Linkage Versus Leverage: Rethinking the International Dimension of Regime Change," *Comparative Politics* 38, no. 4 (2006): 379, doi:10.2307/20434008.

⁷⁶ Там же.

⁷⁷ Thomas Ambrosio, "Catching the 'Shanghai Spirit': How the Shanghai Cooperation Organization Promotes Authoritarian Norms in Central Asia," *Europe-Asia Studies* 60, no. 8 (2008): 1321–44, doi:10.1080/09668130802292143; Thomas Ambrosio, "Constructing a Framework of Authoritarian Diffusion: Concepts, Dynamics, and Future Research," *International Studies Perspectives* 11, no. 4 (2010): 375–92, doi:10.1111/j.1528-3585.2010.00411.x; Weyland, "Crafting Counterrevolution: How Reactionaries Learned to Combat Change in 1848."

⁷⁸ Steven Levitsky and Lucan Way, "International Linkage and Democratization," *Journal of Democracy* 16, no. 3 (2005): 20–34.

⁷⁹ Axel Dreher et al., "Aid, China, and Growth: Evidence from a New Global Development Finance Dataset," *SSRN Electronic Journal*, 2017, doi:10.2139/ssrn.3051044.

⁸⁰ Levitsky and Way, "Linkage Versus Leverage: Rethinking the International Dimension of Regime Change," p. 379.

⁸¹ Bill Marczak et al., "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab*, September 18, 2018, <https://citizenlab.ca/2018/09/hide-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>; Meiya Pico, "Training."

⁸² Crispian Balmer, "China's Xi Looks to Strengthen Italian Ties, Evokes Ancient Trade Routes," *Reuters*, March 22, 2019, <https://uk.reuters.com/article/uk-italy-china-president-idUKKCN1R318O>.

⁸³ Reuters, "Factbox: Draft Italy Belt and Road MOU Has Broad Outlines, Few Specifics," *Reuters*, March 15, 2019, <https://www.reuters.com/article/us-italy-china-mou-factbox-idUSKCN1QW1EB>.

⁸⁴ State Council Information Office - The People's Republic of China, "Journalists from Belt and Road Countries Learn About China," July 13, 2018, http://english.scio.gov.cn/aboutscio/2018-07/13/content_56606453.htm; iiMedia, "'一带一路'沿线国家政府网络监管部门官员代表团到访艾媒," November 14, 2017, <https://www.iimedia.cn/c886/59716.html>.

⁸⁵ Meiya Pico, "Meiya Pico Joined the NELB-ILEC Forum at Lianyungang from Sep 26 to 30," September 21, 2016,

<https://web.archive.org/web/20170217164635/https://meiyapico.com/news/detail-551.html>.

⁸⁶ "Meiya Pico Joined the NELB-ILEC Forum at Lianyungang from Sep 26 to 30," accessed May 1, 2019, <http://web.archive.org/web/20171113105154/https://meiyapico.com/news/detail-551.html>.

⁸⁷ Там же.

⁸⁸ Meiya Pico, "Training."

⁸⁹ Там же.

⁹⁰ Ministry of Foreign Affairs of the Republic of Belarus, "Commonwealth of Independent States," 2019, <http://mfa.gov.by/en/organizations/membership/list/c2bd4cebdf6bd9f9.html>; Radio Free Europe / Radio Liberty, "Ukraine Shuts Down Offices In CIS Member States," *RadioFreeEurope/RadioLiberty*, August 28, 2018, <https://www.rferl.org/a/ukraine-shuts-down-offices-in-cis-member-states/29457859.html>.

⁹¹ This number represents the breadth of diffusion (number of countries exported to) and not the depth (how much was exported to a given country).

⁹² Analytical Business Solutions, "Semantic Archive," n.d., http://www.rustrade.hu/07_Kommercheskie_predlojenia_i_zaprozi/07_01_Predlojenia_ross_expo rt/07_01_01_Tovar/07_01_01_16_Tovari/Semantic%20Archive%20presentation.compressed.pdf.

⁹³ Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*, First (New York: PublicAffairs, 2015).

⁹⁴ VAS Experts, "About Us."

⁹⁵ Peter Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia" (Access Now, 2013), https://web.archive.org/web/20160419101818/https://s3.amazonaws.com/access.3cdn.net/279b95d57718f05046_8sm6ivg69.pdf; Privacy International, "Private Interests: Monitoring Central Asia," November 2014, <https://privacyinternational.org/report/837/private-interests-monitoring-central-asia>.

⁹⁶ Analytical Business Solutions, "Semantic Archive."

⁹⁷ Andrei Soldatov and Irina Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You," *WIRED*, December 21, 2012, <https://www.wired.com/2012/12/russias-hand/>.

⁹⁸ Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.

⁹⁹ VAS Experts, "About Us"; Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia."

¹⁰⁰ Borogan and Soldatov, "Just Business."

¹⁰¹ State Information Center, "Profiles - Belt and Road Portal," accessed July 12, 2019, https://eng.yidaiyilu.gov.cn/info/iList.jsp?cat_id=10076&cur_page=1.

¹⁰² Mercator Institute for China Studies, "Mapping the Belt and Road Initiative: This Is Where We Stand," June 7, 2018, <https://www.merics.org/en/bri-tracker/mapping-the-belt-and-road-initiative>.

¹⁰³ Alessandro Cozzi, "Smart Cities: Envisioning a Sustainable Future," *International Telecommunications Union*, June 18, 2014, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/Documents/SSC-Genoa-Italy-17-20-jun-2014/PPT/Pres3_Cozzi_Alessandro-77

18June2014_Smart_City(Huawei).pdf; Hikvision, "Hikvision Enhances Suez Governorate's Bus Fleet Operation," April 17, 2018, <https://www.hikvision.com/en/Press/Success-Stories/Transportation/Hikvision-enhances-Suez-Governorates-bus-fleet-operation>.

¹⁰⁴ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

¹⁰⁵ Meiya Pico, "The Assistant Minister of Interior and the Director of Information and Communication Bureau of Egypt, Mr. Ahmed Mostafa Visited Meiya Pico.," November 24, 2017, https://web.archive.org/web/20190625190652/https://www.meiyapico.com/the-assistant-minister-of-interior-and-the-director-of-information-and-communication-bureau-of-egypt-mr-ahmed-mostafa-visited-meiya-pico_n11.

¹⁰⁶ The Economic Times, "China, Egypt Sign Strategic Partnership Agreement," *The Economic Times*, December 24, 2014, <https://economictimes.indiatimes.com/news/international/business/china-egypt-sign-strategic-partnership-agreement/articleshow/45629765.cms?from=mdr>.

¹⁰⁷ Al-Masry Al-Youm, "Egyptian Parliament Approves Law to Combat Cybercrime," *Egypt Independent*, May 15, 2018, <https://www.egyptindependent.com/egyptian-parliament-approves-law-to-combat-cybercrime/>.

¹⁰⁸ Steve Stecklow, Farnaz Fassihi, and Loretta Chao, "Chinese Tech Giant Aids Iran," *Wall Street Journal, Eastern Edition; New York, N.Y.*, October 27, 2011, <https://www.wsj.com/articles/SB10001424052970204644504576651503577823210>.

¹⁰⁹ Steve Stecklow, "Special Report: Chinese Firm Helps Iran Spy on Citizens," *Reuters*, March 22, 2012, <https://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322>.

¹¹⁰ Center for Human Rights in Iran, "China to Help Iran Implement Its Closed National Internet," *Center for Human Rights in Iran*, January 21, 2014, <http://www.iranhumanrights.org/2014/01/china-iran-internet/>.

¹¹¹ Al Jazeera, "Iran Releases Messaging App Soroush to Replace Telegram," April 26, 2018, <https://www.aljazeera.com/news/2018/04/iran-releases-messaging-app-soroush-replace-telegram-180426112935318.html>.

¹¹² Center for Human Rights in Iran, "China to Help Iran Implement Its Closed National Internet."

¹¹³ Zhou Yuan and Zhihao Zhang, "China Boosts Soft Power by Training Foreign Journalists," *Chinadaily*, October 17, 2016, http://www.chinadaily.com.cn/china/2016-10/17/content_27077588.htm.

¹¹⁴ Там же.

¹¹⁵ Meiya Pico, "Training."

¹¹⁶ BOTS team, "AFSB First in Malaysia to Integrate Body-Worn Cameras with Facial Recognition Technology," *New Straits Times*, April 16, 2018, <https://www.nst.com.my/lifestyle/bots/2018/04/358122/afsb-first-malaysia-integrate-body-worn-cameras-facial-recognition>.

¹¹⁷ Liz Lee, "Alibaba to Take on Kuala Lumpur's Traffic in First Foreign Project," *Reuters*, January 29, 2018, <https://www.reuters.com/article/us-alibaba-malaysia-idUSKBN1FI0QV>.

¹¹⁸ Yiswaree Palansamy, "Dr M: Taking China's Side? It's Free Speech," *Malay Mail*, June 24, 2019, <https://www.malaymail.com/news/malaysia/2019/06/24/dr-m-taking-chinas-side-its-free-speech/1765086>.

¹¹⁹ Abdul Aziz Harun Bernama, "DPM: Chinese Crime-Fighting Methods Worth Emulating," *78* January 15, 2017, <https://www.malaysiakini.com/news/369309>.

¹²⁰ Radio Free Europe / Radio Liberty, "Q&A: Russia, China Swapping Cybersecurity, Censorship Tips," *RadioFreeEurope/RadioLiberty*, accessed April 30, 2019, <https://www.rferl.org/a/russia-china-swapping-cybersecurity-censorship-tips-internet/28155171.html>.

¹²¹ Seddon and Foy, "Russian Technology."

¹²² Meiya Pico, "Training."

¹²³ Huawei Enterprise, "Huawei Helps Saint Petersburg Become a Safe City," *Facebook*, July 29, 2014, <https://www.facebook.com/huaweiit/photos/a.1433359283549278/1521750881376784/?type=3>.

¹²⁴ Там же.

¹²⁵ Cozzi, "Smart Cities: Envisioning a Sustainable Future."

¹²⁶ Dahua Technology, "Dahua IP Megapixel Solution Secures Government Office in Tanzania," April 3, 2015, <https://www.dahuasecurity.com/newsEvents/successStories/51/30>.

¹²⁷ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

¹²⁸ Banzi, "Tanzania."

¹²⁹ Hikvision, "Hikvision Protects Ministry of Commerce (MOC) Thailand," June 24, 2010, <https://www.hikvision.com/en/Press/Success-Stories/Government/305528969213861>.

¹³⁰ Hikvision, "Hikvision Helping Bangkok's Police Force Stay Ahead of the Curve-Hikvision," July 11, 2012, <https://www.hikvision.com/en/Press/Success-Stories/Government/305528970582113>.

¹³¹ SmartCitiesWorld, "Huawei Helps to Realise 'Thailand 4.0,'" *Smart Cities World*, June 5, 2017, <https://www.smartcitiesworld.net/connectivity/connectivity/huawei-helps-to-realise-thailand-40>.

¹³² Meiya Pico, "Training"; Yuan and Zhang, "China Boosts Soft Power by Training Foreign Journalists."

¹³³ Doug Bernard, "Thailand Set to Build China-like Internet Firewall," *VOA*, September 28, 2015, <https://www.voanews.com/a/thailand-set-to-build-china-like-internet-firewall/2982650.html>.

¹³⁴ Reuters, "Thailand Scraps Unpopular Internet 'Great Firewall' Plan," *Reuters*, October 15, 2015, <https://www.reuters.com/article/us-thailand-internet-idUSKCN0S916I20151015>; Scott Ikeda, "Does the New Thailand Cybersecurity Law Go Too Far?," *CPO Magazine*, March 10, 2019, <https://www.cpomagazine.com/data-privacy/does-the-new-thailand-cybersecurity-law-go-too-far/>; Nithin Coca, "Tourism from China Provokes an Internet Crackdown in Thailand," *Coda Story*, March 12, 2019, <https://codastory.com/authoritarian-tech/tourism-from-china-provokes-an-internet-crackdown-in-thailand/>.

¹³⁵ Yasiin Mugerwa, "China to Help Uganda Fight Internet Abuse," *Daily Monitor*, July 26, 2017, <https://www.monitor.co.ug/News/National/China-Uganda-Internet-Evelyn-Anite-Africa-Internet-Users/688334-4032626-u1l61r/index.html>.

¹³⁶ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

¹³⁷ Unwanted Witness, "Chinese Firm Supplies 900 Surveillance Cameras to Uganda," August 3, 2018, <https://www.unwantedwitness.org/chinese-firm-supplies-900-surveillance-cameras-to-uganda/>.

¹³⁸ Parkinson, Bariyo, and Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents."

¹³⁹ Stephen Kafeero, "Government in New Move to Control Internet," *Daily Monitor*, June 29, 2019, <https://web.archive.org/web/20190710074146/https://www.monitor.co.ug/News/National/Government-new-move-control-Internet/688334-5175382-vbwvsj/index.html/>.

¹⁴⁰ *Zambian Watchdog*, "Huawei Completes Installing Hacking Devices on All Internet Service Providers in Zambia," *Zambian Watchdog*, September 2, 2013, <https://www.zambiawatchdog.com/huawei-completes-installing-hacking-devices-on-all-internet-service-providers-in-zambia/>.

¹⁴¹ Parkinson, Bariyo, and Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents."

¹⁴² Huawei, "Huawei Smart City Overview Presentation," *Huawei Enterprise*, 2018, <https://e.huawei.com/en/material/onLineView?MaterialID=02ad4d5ab608492ea24659ec667f04bd>.

¹⁴³ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

¹⁴⁴ Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain."

¹⁴⁵ Reporters Without Borders, "All Communications Can Now Be Intercepted under New Law Signed by Mugabe," August 6, 2007, <https://rsf.org/en/news/all-communications-can-now-be-intercepted-under-new-law-signed-mugabe>.

¹⁴⁶ Hongpei Zhang, "Chinese Facial ID Tech to Land in Africa," *Global Times*, May 17, 2018, <http://www.globaltimes.cn/content/1102797.shtml>.

¹⁴⁷ Amy Hawkins, "Beijing's Big Brother Tech Needs African Faces," *Foreign Policy*, July 24, 2018, <https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/>.

¹⁴⁸ Xiaoling Zhang, Herman Wasserman, and Winston Mano, "China's Expansion of Influence in Africa: Projection, Perception and Prospects in Southern African Countries," *South African Journal for Communication Theory and Research* 42, no. 1 (March 17, 2016): 1–22.

¹⁴⁹ Towindo, "Government to Regulate Social Media."

¹⁵⁰ Там же.

¹⁵¹ Stephen B Kaplan and Michael Penfold, "China-Venezuela Economic Relations: Hedging Venezuelan Bets with Chinese Characteristics," 2019, https://www.wilsoncenter.org/sites/default/files/china-venezuela_relations_final.pdf.

¹⁵² Angus Berwick, "A New Venezuelan ID, Created with China's ZTE, Tracks Citizen Behavior," *Reuters*, November 14, 2018, <https://www.reuters.com/investigates/special-report/venezuela-zte/>.

¹⁵³ Там же.

¹⁵⁴ Samantha Hoffman, "Social Credit," *Australian Strategic Policy Institute*, June 28, 2018, <https://www.aspi.org.au/report/social-credit>.

¹⁵⁵ Huawei, "Huawei Smart City Solution"; Álvaro Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets" (Institut Barcelona d'Estudis Internacionals (IBEI), 2017), https://www.ibeai.org/surveillance-smart-technologies-and-the-development-of-safe-city-solutions-the-case-of-chinese-ict-firms-and-their-international-expansion-to-emerging-markets_112561.pdf; Ryan Mallett-Outtrim, "30,000 More Security Cameras and 17,000 Less Guns on Venezuelan Streets," *Venezuelanalysis.Com*, November 27, 2013, <https://venezuelanalysis.com/news/10198>.

¹⁵⁶ VEN 911, "#Ahora | Personal De Huawei Refuerza Conocimientos Al Personal De Tecnología Del #VEN911 Barinas Para El Mantenimiento De Data Center #Dialogoproductivoenmarcha," June 4, 2018, 911, <https://twitter.com/VEN911Oficial/status/1003657444264996864>.

¹⁵⁷ Borogan and Soldatov, "Just Business."

¹⁵⁸ Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917.

¹⁵⁹ Meiya Pico, "Training"; Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance."

¹⁶⁰ Gooood, "Baise Executive Leadership Academy, China By ECADI," September 13, 2017, <https://www.gooood.cn/baise-executive-leadership-academy-by-ecadi.htm>.

¹⁶¹ Mozur, Kessel, and Chan, "Made in China, Exported to the World: The Surveillance State."

¹⁶² Joan Tilouine and Ghalia Kadiri, "A Addis-Abeba, le Siège de l'Union Africaine Espionné par Pékin," *Le Monde*, January 26, 2018, http://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

¹⁶³ Leo Kelion and Sajid Iqbal, "Huawei Kit Pulled from Pakistan CCTV System," April 8, 2019, sec. Technology, <https://www.bbc.com/news/technology-47856098>.

¹⁶⁴ Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."

¹⁶⁵ People's Daily, "China-Designed Big Data System Aids Angola's Intelligent Governance," August 23, 2018, <https://web.archive.org/web/20190202234913/http://www.eurasiainfo.ch/en/china-designed-big-data-system-aids-angolas-intelligent-governance/>.

¹⁶⁶ Christian M. Wade, "Massachusetts Considers Bill to Limit Facial Recognition," February 11, 2019, <https://www.govtech.com/policy/Massachusetts-Considers-Bill-to-Limit-Facial-Recognition.html>.

¹⁶⁷ Kate Conger, Richard Fausset, and Serge F. Kovalski, "San Francisco Bans Facial Recognition Technology," *The New York Times*, May 16, 2019, sec. U.S., <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>.

¹⁶⁸ Marczak et al., "HIDE AND SEEK"; Dalek et al., "Planet Netsweeper."

¹⁶⁹ BBC, "Australia Data Encryption Laws Explained," December 7, 2018, sec. Australia, <https://www.bbc.com/news/world-australia-46463029>.

¹⁷⁰ Zack Whittaker, "'Five Eyes' Governments Call on Tech Giants to Build Encryption Backdoors — or Else," *TechCrunch*, September 3, 2018, <http://social.techcrunch.com/2018/09/03/five-eyes-governments-call-on-tech-giants-to-build-encryption-backdoors-or-else/>.

¹⁷¹ Urs Gasser et al., "Don't Panic: Making Progress on the 'Going Dark' Debate," February 1, 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

¹⁷² Mozur, Kessel, and Chan, "Made in China, Exported to the World: The Surveillance State."

¹⁷³ "Д" обозначает ждемократию, "Г" обозначает гибридный реджим и "А" обозначает авторитарный режимefers to democracy, "H" to hybrid regime, and "A" to authoritarian regime.

¹⁷⁴ Huawei, "Huawei Smart City Solution."

¹⁷⁵ Borogan and Soldatov, "Just Business."

¹⁷⁶ People's Daily, "China-Designed Big Data System Aids Angola's Intelligent Governance," *EurAsia Info*, August 23, 2018, <http://www.eurasiainfo.ch/en/china-designed-big-data-system-aids-angolas-intelligent-governance/>.

¹⁷⁷ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

¹⁷⁸ Stabroek News, "China Launches Press Programme to Improve Ties with Caribbean."

¹⁷⁹ Hikvision, "Hikvision and Argentina."

¹⁸⁰ Meiya Pico, "Training."

¹⁸¹ Там же.

¹⁸² Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance."

¹⁸³ Trend News Agency, "Китайская Huawei построит 'Умный город' в Баку," *Trend.Az*, March 18, 2017, <https://www.trend.az/business/it/2733661.html>.

¹⁸⁴ VAS Experts, "About Us."

¹⁸⁵ Rafal Rohozinski and Vesselina Haralampieva, "Internet Filtering in the Commonwealth of Independent States 2006-2007," *OpenNet Initiative*, 2007, <https://opennet.net/studies/cis2007>.

¹⁸⁶ Zhang, "China-Caribbean Press Center Launched."

¹⁸⁷ Yuan and Zhang, "China Boosts Soft Power by Training Foreign Journalists."

¹⁸⁸ Zhang, "China-Caribbean Press Center Launched."

¹⁸⁹ Freedom House, "Belarus Country Report | Freedom on the Net 2017," November 14, 2017, <https://freedomhouse.org/report/freedom-net/2017/belarus>.

¹⁹⁰ Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.

¹⁹¹ Там же.

¹⁹² Meiya Pico, "Training."

¹⁹³ Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."

¹⁹⁴ Frederick P. W. Gaye, "33 African Journalists Arrive China for Training," *People's Daily*, August 9, 2016, <http://en.people.cn/n3/2016/0809/c90000-9097628.html>.

¹⁹⁵ Hikvision, "World Cup Inspired Security and Hikvision Protect Brazil," January 17, 2012, <https://www.hikvision.com/en/Press/Success-Stories/City-Surveillance/305528876368336>.

¹⁹⁶ Xinhua, "China Donates Traffic Cameras, Anti-Cybercrime Equipment to Cambodia - People's Daily Online," *Xinhua*, December 22, 2015, <http://en.people.cn/n/2015/1222/c90000-8994022.html>.

¹⁹⁷ Meiya Pico, "Training."

¹⁹⁸ Huawei, "Huawei Tetra over ELTE," 2014, http://btg.org/wp-content/uploads/2014/11/Huawei-Tetra-over-eLTE_BTG.pdf.

¹⁹⁹ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

²⁰⁰ Там же.

²⁰¹ Там же.

²⁰² Huawei, "Huawei Announces Safe City Compact Solution to Protect Citizens in Small and Medium Cities," *Huawei Enterprise*, August 29, 2018, <https://e.huawei.com/en/news/global/2018/201808391810>.

²⁰³ Alexander Gabuev, "How China and Russia See the Internet," *World Economic Forum*, December 16, 2015, <https://www.weforum.org/agenda/2015/12/how-china-and-russia-see-the-internet/>.

²⁰⁴ Huawei, "Huawei Announces Safe City Compact Solution to Protect Citizens in Small and Medium Cities."

²⁰⁵ Borogan and Soldatov, "Just Business."

²⁰⁶ Meiya Pico, "Training."

²⁰⁷ Protei, "NEWS - Telecommunication Solutions," 2015, <http://www.protei.com/news/>.

²⁰⁸ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

-
- ²⁰⁹ Huawei, "Safe City: Abidjan, Côte D'Ivoire," *Huawei Enterprise*, accessed May 1, 2019, <https://e.huawei.com/en/videos/global/2018/201809121118>.
- ²¹⁰ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²¹¹ Xynou, Filastò, and Basso, "Measuring Internet Censorship in Cuba's ParkNets."
- ²¹² Protei, "Past Events."
- ²¹³ Stabroek News, "China Launches Press Programme to Improve Ties with Caribbean."
- ²¹⁴ Jun Mai, "Ecuador Is Fighting Crime Using Chinese Surveillance Technology," *South China Morning Post*, January 22, 2018, <https://www.scmp.com/news/china/diplomacy-defence/article/2129912/ecuador-fighting-crime-using-chinese-surveillance>.
- ²¹⁵ SpeechPro, "SpeechPro Deploys the World's First Voice and Face Biometrics System in Ecuador," December 17, 2012, <https://speechpro-usa.com/media/news/2012-12-17>.
- ²¹⁶ VEN 911, "#Ahora | Personal De Huawei Refuerza Conocimientos Al Personal De Tecnología Del #VEN911 Barinas Para El Mantenimiento De Data Center #Dialogoproductivoenmarcha," 91.
- ²¹⁷ Cozzi, "Smart Cities: Envisioning a Sustainable Future."
- ²¹⁸ Al-Youm, "Egyptian Parliament Approves Law to Combat Cybercrime."
- ²¹⁹ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²²⁰ Там же.
- ²²¹ Human Rights Watch, "Ethiopia: Telecom Surveillance Chills Rights," *Human Rights Watch*, March 25, 2014, <https://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights>.
- ²²² Sanja Kelly, Sarah Cook, and Mai Truong, "Freedom on the Net 2012: A Global Assessment of Internet and Digital Media" (Freedom House, September 24, 2012), <https://freedomhouse.org/sites/default/files/FOTN%202012%20summary%20of%20findings.pdf>.
- ²²³ Xinhua, "Huawei Helps France Create 'Safe City' -," 2017, http://www.xinhuanet.com/world/2017-02/10/c_1120445581.htm.
- ²²⁴ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²²⁵ Huawei Enterprise, "Gelsenkirchen: A Small, Smart City with Big Plans," *Huawei Enterprise*, 2017, <https://e.huawei.com/us/case-studies/global/2017/201709071445>.
- ²²⁶ Huawei, "Huawei Tetra over ELTE."
- ²²⁷ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²²⁸ Zhang, "China-Caribbean Press Center Launched."
- ²²⁹ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²³⁰ Zhang, "China-Caribbean Press Center Launched."
- ²³¹ Huawei, "Huawei Smart City Overview Presentation."
- ²³² Borogan and Soldatov, "Just Business."
- ²³³ Meiya Pico, "Training."
- ²³⁴ Huawei Enterprise, "Safe City: Bandung Indonesia," *Huawei Enterprise*, accessed January 20, 2019, <https://e.huawei.com/en/videos/global/2018/201804101042>.
- ²³⁵ Meiya Pico, "Training."
- ²³⁶ Stecklow, Fassihi, and Chao, "Chinese Tech Giant Aids Iran."
- ²³⁷ Al Jazeera, "Iran Releases Messaging App Soroush to Replace Telegram."
- ²³⁸ Center for Human Rights in Iran, "China to Help Iran Implement Its Closed National Internet."

-
- ²³⁹ Xinhua, "China's Huawei Helps Promote Security in Iraq's Capital via 'Safe City Solution' Project," July 15, 2019, http://www.xinhuanet.com/english/2019-03/08/c_137876838.htm.
- ²⁴⁰ Hikvision, "Hikvision Provides a Safe and Secure Harbour for Dun Laoghaire," April 8, 2015, <https://www.hikvision.com/en/Press/Success-Stories/Transportation/305529081472324>.
- ²⁴¹ Hikvision, "Total Control for Jordan's House of Parliament."
- ²⁴² Huawei Enterprise, "Smart City."
- ²⁴³ Zhang, "China-Caribbean Press Center Launched."
- ²⁴⁴ Privacy International, "Private Interests: Monitoring Central Asia."
- ²⁴⁵ Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."
- ²⁴⁶ Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.
- ²⁴⁷ Meiya Pico, "Training."
- ²⁴⁸ Edith Muthethya, "New Vision for Big Data: Safe Cities," *China Daily Europe*, November 4, 2016, http://europe.chinadaily.com.cn/epaper/2016-11/04/content_27269942.htm.
- ²⁴⁹ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²⁵⁰ Caravanserai, "Bishkek to Install Facial Recognition System as Part of Smart City Project," *Caravanserai*, February 9, 2018, http://central.asia-news.com/en_GB/articles/cnmi_ca/newsbriefs/2018/02/09/newsbrief-02.
- ²⁵¹ Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."
- ²⁵² Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.
- ²⁵³ Meiya Pico, "Training."
- ²⁵⁴ Huawei Enterprise, "Safe City Service Brings the Future to Laos," *Huawei Enterprise*, April 3, 2015, <https://e.huawei.com/au/case-studies/global/2015/201504030937>.
- ²⁵⁵ He, "In a Remote Corner of China, Beijing Is Trying to Export Its Model by Training Foreign Officials the Chinese Way."
- ²⁵⁶ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²⁵⁷ Там же.
- ²⁵⁸ Paul Sonne and Margaret Coker, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, sec. World News, <https://www.wsj.com/articles/SB10001424053111904199404576538721260166388>.
- ²⁵⁹ VAS Experts, "About Us."
- ²⁶⁰ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²⁶¹ BOTS team, "AFSB First in Malaysia to Integrate Body-Worn Cameras with Facial Recognition Technology."
- ²⁶² Bernama, "DPM: Chinese Crime-Fighting Methods Worth Emulating."
- ²⁶³ Meiya Pico, "Training."
- ²⁶⁴ SpeechPro, "Maldives Police Chose the Expert Suite IKAR Lab by Speech Technology Center," September 26, 2016, <https://speechpro-usa.com/media/news/2016-09-26>.
- ²⁶⁵ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²⁶⁶ Republic of Mauritius, "Sixth National Assembly - Parliamentary Debates," 2018, <http://mauritiusassembly.govmu.org/English/hansard/Documents/2018/hansard0718.pdf>.

-
- ²⁶⁷ Bai Jianhua, "ICT Builds Safe Cities," *Huawei Enterprise*, accessed January 20, 2019, https://e.huawei.com/us/publications/global/ict_insights/201701051027/special-report/201701051524.
- ²⁶⁸ SpeechPro, "World's First Nationwide Voice Identification System Deployed in Mexico by Speech Technology Center (Russia)," March 6, 2010, <https://speechpro-usa.com/media/news/2010-06-03>.
- ²⁶⁹ Huawei, "Huawei Smart City Overview Presentation."
- ²⁷⁰ Rohozinski and Haralampieva, "Internet Filtering in the Commonwealth of Independent States 2006-2007."
- ²⁷¹ Xu Li, "Making Sense of Sensetime," *Jumpstart*, April 6, 2018, <https://jumpstartmag.com/making-sense-of-sensetime/>.
- ²⁷² Meiya Pico, "Forensic MagiCube Got High Comments in Mongolia - Web.Archive," November 13, 2017, <https://web.archive.org/web/20171113141645/https://meiyapico.com/news/detail-533.html>.
- ²⁷³ Huawei, "Marrakesh: Safe City," *Huawei Enterprise*, 2018, <https://e.huawei.com/en/videos/industries/2018/201812060902>.
- ²⁷⁴ Meiya Pico, "Training."
- ²⁷⁵ Cozzi, "Smart Cities: Envisioning a Sustainable Future."
- ²⁷⁶ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²⁷⁷ Asmag, "Yangon Goes Live with Hikvision Traffic Management Solution," *Asmag*, September 27, 2017, <https://www.asmag.com/showpost/23776.aspx>.
- ²⁷⁸ He, "In a Remote Corner of China, Beijing Is Trying to Export Its Model by Training Foreign Officials the Chinese Way."
- ²⁷⁹ SpeechPro, "Nepalese Law Enforcement Chooses SpeechPro for Audio Forensics and Voice Identification," August 11, 2013, <https://speechpro-usa.com/media/news/2013-11-08>.
- ²⁸⁰ Huawei, "Huawei Tetra over ELTE."
- ²⁸¹ VAS Experts, "About Us."
- ²⁸² Cozzi, "Smart Cities: Envisioning a Sustainable Future."
- ²⁸³ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²⁸⁴ Cozzi, "Smart Cities: Envisioning a Sustainable Future."
- ²⁸⁵ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ²⁸⁶ Huawei, "Huawei Tetra over ELTE."
- ²⁸⁷ Xdyanmix, "Huawei Safe City," *Xdynamix Media Communications*, 2018, <http://xdynamix.com/portfolio/huawei-safe-city/>.
- ²⁸⁸ The International News, "Pakistani Journalists Complete Ten Month Training Programme in China," December 13, 2018, <https://www.thenews.com.pk/latest/405387-pakistani-journalists-complete-ten-month-training-programme-in-china>.
- ²⁸⁹ Protei, "News and Events - Protei MENA."
- ²⁹⁰ Cardenal, "China in Latin America: Understanding the Inventory of Influence."
- ²⁹¹ Huawei Enterprise, "Making Manila's 'Crown Jewel' a Safe City — Huawei Case Studies," *Huawei Enterprise*, 2017, <https://e.huawei.com/en/case-studies/global/2017/201704261658>.
- ²⁹² Lilian Mellejor, "Andanar Sends off 21 Journalists, Info Officers to China," May 16, 2018, <http://www.pna.gov.ph/articles/1035427>.
- ²⁹³ Huawei, "Huawei Tetra over ELTE."

-
- ²⁹⁴ Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
- ²⁹⁵ Huawei Enterprise, "Huawei Helps Saint Petersburg Become a Safe City."
- ²⁹⁶ Soldatov and Borogan, "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact."
- ²⁹⁷ Meiya Pico, "Training."
- ²⁹⁸ Gaye, "33 African Journalists Arrive China for Training."
- ²⁹⁹ Huawei Enterprise, "Yanbu: A Smart Industrial Oil Kingdom City," *Huawei Enterprise*, accessed January 20, 2019, https://e.huawei.com/us/publications/global/ict_insights/201708310903/manufacturing/201712061133.
- ³⁰⁰ Borogan and Soldatov, "Just Business."
- ³⁰¹ Meiya Pico, "Training."
- ³⁰² Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
- ³⁰³ Huawei Enterprise, "Huawei Safe City Solution: Safeguards Serbia," *Huawei Enterprise*, accessed January 20, 2019, <https://web.archive.org/web/20190329132454/https://e.huawei.com/en/case-studies/global/2018/201808231012>.
- ³⁰⁴ Gaye, "33 African Journalists Arrive China for Training."
- ³⁰⁵ Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
- ³⁰⁶ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ³⁰⁷ Jianhua, "ICT Builds Safe Cities."
- ³⁰⁸ Borogan and Soldatov, "Just Business."
- ³⁰⁹ Meiya Pico, "Training."
- ³¹⁰ Hikvision, "Sea Point Sees Two-Thirds Crime Drop After Hikvision Cameras Deployed," May 8, 2015, <https://www.hikvision.com/en/Press/Success-Stories/Transportation/305529081636891>.
- ³¹¹ Meiya Pico, "Training."
- ³¹² Hikvision, "Company Profile-Hikvision," accessed January 21, 2019, <https://www.hikvision.com/en/Corporate/Company-Profile>.
- ³¹³ Yuan and Zhang, "China Boosts Soft Power by Training Foreign Journalists."
- ³¹⁴ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ³¹⁵ Huawei Enterprise, "Spain Enhances Smart City with ELTE Solution."
- ³¹⁶ Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
- ³¹⁷ Bandula Sirimanna, "Chinese Here for Cyber Censorship," *The Sunday Times*, February 14, 2010, https://web.archive.org/web/20100215081800/www.sundaytimes.lk/100214/News/nws_02.html.
- ³¹⁸ Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
- ³¹⁹ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ³²⁰ Zhang, "China-Caribbean Press Center Launched."
- ³²¹ Huawei Enterprise, "Safe City Improves Traffic, Cuts Crime," *Huawei Enterprise*, April 3, 2015, <https://e.huawei.com/sg/case-studies/global/2015/201504031050>.

-
- ³²² Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia."
- ³²³ Meiya Pico, "Training."
- ³²⁴ Cozzi, "Smart Cities: Envisioning a Sustainable Future."
- ³²⁵ Banzi, "Tanzania."
- ³²⁶ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ³²⁷ SmartCitiesWorld, "Huawei Helps to Realise 'Thailand 4.0.'"
- ³²⁸ Borogan and Soldatov, "Just Business."
- ³²⁹ Bernard, "Thailand Set to Build China-like Internet Firewall."
- ³³⁰ Yuan and Zhang, "China Boosts Soft Power by Training Foreign Journalists."
- ³³¹ Sohu, "中国电子进出口：扎根拉美，推动信息化能力“走出去”，" October 9, 2017, www.sohu.com/a/197072125_444154.
- ³³² Zhang, "China-Caribbean Press Center Launched."
- ³³³ Cozzi, "Smart Cities: Envisioning a Sustainable Future."
- ³³⁴ Borogan and Soldatov, "Just Business."
- ³³⁵ Meiya Pico, "Training."
- ³³⁶ Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia."
- ³³⁷ Meiya Pico, "Training."
- ³³⁸ Unwanted Witness, "Chinese Firm Supplies 900 Surveillance Cameras to Uganda."
- ³³⁹ Kafeero, "Government in New Move to Control Internet."
- ³⁴⁰ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."
- ³⁴¹ Liga.net, "Smart City - Города с Разумом," accessed May 1, 2019, http://www.liga.net/projects/smart_city/.
- ³⁴² Soldatov and Borogan, *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*.
- ³⁴³ Там же.
- ³⁴⁴ Huawei Enterprise, "Huawei Partners with Dubai Airports to Build a Smart Airport," *Huawei Enterprise*, accessed January 20, 2019, https://e.huawei.com/us/publications/global/ict_insights/201708310903/transportation-logistics/201708311040.
- ³⁴⁵ Hikvision, "Hikvision Helps London Borough Build Extensive CCTV Solution," December 11, 2013, <https://www.hikvision.com/en/Press/Success-Stories/City-Surveillance/305528877699609>.
- ³⁴⁶ Meiya Pico, "Training."
- ³⁴⁷ Huawei, "Huawei Tetra over ELTE."
- ³⁴⁸ Ryan Gallagher, "Watch Your Tongue: Law Enforcement Speech Recognition System Stores Millions of Voices," *Slate Magazine*, September 20, 2012, <https://slate.com/technology/2012/09/speechpro-voicegrid-nation-voice-recognition-software-for-use-by-law-enforcement.html>.
- ³⁴⁹ Lim and Bergin, "Inside China's Audacious Plan for Global Media Dominance."
- ³⁵⁰ Artigas, "Surveillance, Smart Technologies and the Development of Safe City Solutions: The Case of Chinese ICT Firms and Their International Expansion to Emerging Markets."
- ³⁵¹ Privacy International, "Private Interests: Monitoring Central Asia."
- ⁸⁷
³⁵² Soldatov and Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You."

³⁵³ Borogan and Soldatov, "Just Business."

³⁵⁴ Meiya Pico, "Training."

³⁵⁵ Mallett-Outtrim, "30,000 More Security Cameras and 17,000 Less Guns on Venezuelan Streets."

³⁵⁶ Berwick, "A New Venezuelan ID, Created with China's ZTE, Tracks Citizen Behavior."

³⁵⁷ VEN 911, "#Ahora | Personal De Huawei Refuerza Conocimientos Al Personal De Tecnología Del #VEN911 Barinas Para El Mantenimiento De Data Center #Dialogoproductivoenmarcha."

³⁵⁸ Trinh Huu Long, "Vietnam's Cybersecurity Draft Law: Made in China?," November 8, 2017, <https://www.thevietnamese.org/2017/11/vietnams-cyber-security-draft-law-made-in-china/>.

³⁵⁹ He, "In a Remote Corner of China, Beijing Is Trying to Export Its Model by Training Foreign Officials the Chinese Way."

³⁶⁰ Borogan and Soldatov, "Just Business."

³⁶¹ Huawei, "Huawei Smart City Overview Presentation."

³⁶² Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain."

³⁶³ Gaye, "28 African Journalists Complete 10-Month Media Fellowship in China."

³⁶⁴ Zhang, "Chinese Facial ID Tech to Land in Africa."

³⁶⁵ Towindo, "Government to Regulate Social Media."

³⁶⁶ Zhang, Wasserman, and Mano, "China's Expansion of Influence in Africa: Projection, Perception and Prospects in Southern African Countries."